Indice

CAPITOLO 1
Navigazione web 5

CAPITOLO 2
Posta elettronica 7

CAPITOLO 3
Comunità virtuali 17

CAPITOLO 4
Acquisti online 27

CAPITOLO 5
P2P 39

Navigazione web

COSA SIGNIFICA NAVIGARE NEL WEB

Internet è un insieme vastissimo di documenti testuali. Ai suoi esordi Internet era costituita unicamente di testo e indici ipertestuali di testi. Con il passare del tempo le cose si sono evolute, sono stati introdotti nuovi servizi e funzionalità, facendo di Internet una risorsa fondamentale per la società, un vero e proprio "villaggio globale".

Il web (da WWW=World Wide Web) si basa sull'infrastruttura di Internet per realizzare una grande risorsa di informazioni.

Dietro i siti web ci sono diversi livelli di strutture dati, ma tutto ciò resta quasi completamente nascosto all'utente, interessato soprattutto all'informazione contenuta in essi.

È importante che i siti web soddisfino i requisiti fondamentali dell'usabilità:

- l'utilità
- la facilità di apprendimento
- l'efficienza
- la soddisfazione
- la facilità di ricordo

Queste sono caratteristiche indispensabili per favorire la navigazione web. Anche per gli utenti diversamente abili la navigazione web deve essere un privilegio di cui non ci si

può privare.

Per questo nella progettazione e realizzazione di siti web il concetto di accessibilità assume sempre maggiore importanza.

Posta elettronica

COSA È LA POSTA ELETTRONICA

La posta elettronica è una delle più diffuse applicazioni Internet. Essa è asincrona, si possono inviare e leggere i messaggi quando si desidera, senza doversi coordinare con gli orari delle altre persone.

La posta elettronica è veloce, facile da distribuire e poco costosa; inoltre, con essa è possibile comporre messaggi non solo testuali, ma corredati da hyperlink, testi in formato HTML, immagini, suoni, video.

La posta elettronica è un mezzo per trasmettere dei messaggi in tempo reale da un computer ad un altro utilizzando la rete Internet.

Quando un provider concede ad un utente l'accesso ad Internet, gli assegna un identificativo che lo individua in modo univoco nella rete e, in genere, gli mette a disposizione anche una mailbox (casella di posta elettronica) cioè uno spazio fisico sul server dove verranno automaticamente depositati i messaggi a lui diretti.

Il meccanismo di trasmissione della posta è molto semplice:

- quando un utente vuole inviare un messaggio elettronico ad un altro utente, scrive un messaggio sul proprio computer, specificando con esattezza l'indirizzo e-mail del destinatario
- si collega al proprio provider mediante linea telefonica
- trasmette il messaggio

- chiude il collegamento
- il messaggio giunge sul server del provider
- il server lo immette nella rete Internet dei computer, detti “router”i quali, leggendo l'indirizzo di destinazione, instraderanno il messaggio nella rete fino al server del provider presso il quale il destinatario è abbonato
- il messaggio resta a disposizione sul server di arrivo fino a quando il destinatario, collegandosi a sua volta a Internet, ed in particolare alla sua mailbox (casella di posta), non decide di leggerlo.

La casella di posta dell’utente gestisce e mantiene i messaggi che gli vengono spediti. Di regola un messaggio arriva al server di posta del mittente e da qui viaggia fino al server di posta del destinatario, dove viene depositato nella casella di posta. I server di posta devono considerare anche eventuali guasti che possono verificarsi; per questo motivo se il server del mittente non può inviare la posta al server del destinatario, allora mantiene il “messaggio in coda” e proverà ad inviarlo più tardi. I nuovi tentativi vengono fatti di solito ogni 30 minuti; se questi non hanno successo per diversi giorni, il server rimuove i messaggi e notifica il mancato recapito al mittente con un apposito messaggio e-mail.

COME FUNZIONA LA POSTA ELETTRONICA

Per usufruire del servizio di posta elettronica ciascun utente ha la necessità di avere un proprio indirizzo e-mail, e questo è possibile tramite la registrazione presso uno dei molteplici provider di posta, che rappresentano i fornitori del servizio.

I provider sono normalmente accessibili direttamente dal web attraverso il sito corrispondente; essi, all'interno dei

propri server, mettono a disposizione dell'utente registrato uno "spazio di memoria" riservato (la casella di posta elettronica), attraverso cui l'utente riceve e legge i messaggi a lui indirizzati e spedisce verso altri utenti i suoi messaggi.

Il processo di registrazione ad un provider di posta prevede una fase di iscrizione al servizio: oltre ad informazioni generali (dati personali, alcuni dei quali opzionali), all'utente viene richiesto di inserire dati essenziali, quali username e password, necessari per l'accesso al servizio e richiesti ogni qualvolta si desidera usufruirne. Generalmente, nel gergo informatico, username e password vengono riferite come account di posta, che identifica univocamente l'utente nella rete.

Nel fornire i dati di carattere privato (nome, telefono, età, sesso ed altro), è opportuno fare attenzione alla attendibilità del provider che si è scelto e a quanto specificato in materia di trattamento dei dati personali.

I provider di posta mettono a disposizione dei propri clienti indirizzi di posta elettronica gratuiti o in modalità a pagamento, in funzione dei servizi associati o anche in relazione alla dimensione della casella di posta (spazio disponibile).

A supporto del servizio di posta elettronica, un utente possessore di uno o più indirizzi e-mail può leggere, scrivere ed inviare messaggi sul proprio computer attraverso specifici software client (come ad esempio Microspoft Outlook, Microsoft Outlook Express, Mozilla Thunderbird).

Il vantaggio dei client è quello di avere un' unica interfaccia dalla quale gestire, in modo semplice, più indirizzi

semplificando l'utilizzo del servizio attraverso funzionalità aggiuntive: rubrica, correttore grammaticale dei messaggi, meccanismi di formattazione, gestione degli allegati, possibilità di memorizzare sul proprio computer i messaggi provenienti dal server di posta.

Non tutti i provider danno la possibilità di usufruire di un client per l'accesso alla casella postale; spesso l'accesso è consentito solo via web, tramite la connessione al sito fornitore del servizio al servizio.

L'utente, dopo essersi connesso al server di posta tramite il client presente sul PC o direttamente attraverso l'accesso web, e dopo aver fornito le proprie credenziali (username e password) in modo corretto, può accedere al servizio, leggere messaggi ricevuti, crearne di nuovi e spedirli ad altri utenti. Durante questi processi di invio e ricezione, il client ed il server dialogano attraverso Internet utilizzando appositi protocolli di comunicazione:

- POP3 (Post Office Protocol):
- IMAP (Internet Message Access Protocol oppure Interactive Mail Access Protocol)
- SMTP (Simple Mail Transfer Protocol).

PRINCIPALI MINACCE

Per la sua semplicità di utilizzo e diffusione capillare tra gli utenti di Internet, sempre la posta elettronica ha sempre rappresentato uno dei principali vettori per la diffusione di diverse tipologie di minacce e di attacchi di tipo informatico.

Un messaggio "contraffatto" può avere:

- le stesse sembianze di un messaggio normale
- l'indirizzo del mittente può essere "ragionevole" o ben conosciuto dal destinatario
- il contenuto può essere ben scritto risultando del tutto credibile; in alcuni casi può, addirittura, contenere frasi estratte da messaggi effettivamente ricevuti o inviatida un mittente conosciuto.

Attraverso la posta elettronica, ad esempio, è possibile la trasmissione di virus e trojan. I virus, sfruttando soprattutto i file allegati nel messaggio, possono contenere programmi che si installano sul PC del malcapitato, per danneggiarne il sistema, controllarne delle porzioni, copiare informazioni private, replicarsi e diffondersi su altre postazioni non protette.

Spesso i virus, propagandosi attraverso il servizio di posta elettronica, riescono, ad infettare una singola casella di posta, poi a risalire ad altri indirizzi in essa contenuti, spedendo nuovi messaggi con il virus in allegato allo scopo di diffonderlo il più possibile.

Come i virus, i trojan non si diffondono autonomamente ma richiedono un intervento diretto del pirata informatico.

Le funzionalità del trojan sono nascoste all'interno di un programma apparentemente utile; l'utente, installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto, che può contenere qualsiasi istruzione maligna.

I messaggi di posta elettronica vengono sfruttati anche per diffondere messaggi pubblicitari volti alla promozione di prodotti stravaganti o illegali, oppure per pubblicizzare siti web dai contenuti più disparati. Questi messaggi

indesiderati finiscono per intasare le caselle di posta elettronica degli utenti, creando un disservizio conosciuto con il nome di spam.

Lo spam, o spamming, prevede la spedizione simultanea di uno stesso messaggio a centinaia o migliaia di indirizzi di posta elettronica.

In che modo gli spammer si procurano indirizzi? La loro fonte preferita sono i newsgroup, dove si trovano migliaia di messaggi pubblici, ognuno con il mittente chiaramente indicato; utilizzando degli appositi programmi, gli spammer riescono ad estrarre in pochi istanti tutti gli indirizzi dei mittenti dei messaggi.

Un altro esempio che mostra un uso illegale della posta elettronica è rappresentato dal phishing, ovvero la generazione di messaggi fasulli che inducono gli utenti a rivelare informazioni riservate che possono essere utilizzate soprattutto per scopi illeciti (come ad esempio le credenziali di accesso al conto bancario online).

Il fenomeno del phishing è un vero e proprio "furto di identità" mediante la comunicazione elettronica. Un tipico attacco phishing generalmente avviene nel seguente modo: l'utente ignaro riceve un messaggio e-mail che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca); questo messaggio contiene quasi sempre avvisi di problemi verificatisi ad esempio con il conto corrente, invitando l'utente a seguire un link per sistemare la situazione. In realtà il link non del tutto porta al sito web ufficiale, ma ad una copia fittizia simile al sito ufficiale, situata su un server controllato dal

phisher; così l'utente ingannato provvede a fornire i dati personali che verranno catturati per altri scopi, come acquistare beni o trasferire somme di denaro.

Nonostante questo scenario possa prospettare una realtà preoccupante per gli utenti della posta elettronica, esistono oggi delle adeguate contromisure per rendere questo servizio di comunicazione più sicuro ed affidabile.

COME DIFENDERSI

Per difendersi dalle minacce provenienti dal servizio di posta elettronica potrebbe essere sufficiente osservare rigorosamente la seguente indicazione: "non aprire mai messaggi di posta elettronica che presentano una forma non convenzionale (strana)".

Nella sua semplicità questa affermazione racchiude una serie di suggerimenti che dovrebbero indurre l'utente ad evitare possibili inconvenienti. La stranezza dei messaggi può ravvisarsi in diverse caratteristiche.

È consigliabile non prendere in considerazione:

- un mittente non conosciuto, con una struttura (di dominio) non ben riconducibile (es. …@axjcie.uu)
- messaggi con indicazioni nel campo Oggetto che lasciano presagire ad un contenuto di dubbia identificazione, con riferimenti ad argomenti tipo sesso, droghe, facili guadagni…
- la presenza di caratteri non riconoscibili (es. lingua non riconosciuta dal client di posta)

- la ripetizione di più messaggi con lo stesso mittente
- la presenza di file allegati inattesi che contengono applicazioni "eseguibili" non conosciute e che potrebbero essere fonte di inganno.

Prima di cliccare su collegamenti insoliti o dubbi allegati, è sempre meglio contattare il mittente, se conosciuto, per verificarne la corretta provenienza.

In generale, il primo accorgimento da adottare per difendersi dalle minacce di posta elettronica è l'analisi degli elementi che identificano il messaggio, ancor prima della sua apertura: ossia il mittente, l'oggetto e la presenza di allegati.

Altri meccanismi di difesa sono rappresentati da software specializzati al filtraggio del traffico e al controllo del contenuto di e-mail sospette. Tra questi troviamo i software antivirus ed antispam, oggi molto diffusi; sono disponibili versioni sia a pagamento che gratuite, spesso semplici da utilizzare e con un elevato grado di affidabilità, soprattutto se mantenuti costantemente aggiornati.

Per contrastare il diffusissimo fenomeno dello spam, alcuni provider, attraverso un filtraggio di messaggi chiaramente identificabili come spam, impediscono il recapito di una porzione considerevole di posta indesiderata al destinatario. L'utente, invece, deve seguire una sorta di codice comportamentale per la sicurezza:

- Considerare il proprio indirizzo di posta elettronica

come una informazione sensibile e per questo limitarne la diffusione nella rete in modo indiscriminato

- evitare di scrivere il proprio indirizzo di posta in siti di cui non si conosce bene il contenuto, 'autenticità ed il fine per il quale viene effettuata la richiesta
- non pubblicare il proprio indirizzo di posta in chat, blog o altri gruppi di diffusione; i newsgroup, infatti, rappresentano la principale fonte da cui estrapolare indirizzi e-mail allo scopo di spamming. Per evitare ciò, è conveniente camuffare il proprio indirizzo inserendovi un elemento estraneo, in modo da ingannare i programmi dello spammer, ma permettere agli altri utenti di accorgersi del trucco e risalire comunque al vero indirizzo; ad esempio un indirizzo del tipo "user@dominio.it" può essere camuffato in "user@EVITASPAMdominio.it".

Per contrastare il fenomeno dello spam modo efficace è quindi utile:

- applicare filtri anti-spam
- eliminare i messaggi sospetti
- non cliccare su collegamenti o aprire allegati in messaggi sospetti
- non rispondere a messaggi di spam

Per contrastare il phishing, ovvero il pericolo che qualcuno possa entrare impropriamente in possesso di dati riservati, è utile adottare dei comportamenti precauzionali:

- Non rispondere a messaggi di posta elettronica che richiedono l'invio di informazioni personali o di

carattere finanziario (come ad esempio il proprio numero di conto corrente o il numero di carta di credito). Una banca, conoscendo i rischi di queste minacce, non chiederà mai ai propri clienti di inviare via e-mail informazioni tanto riservate.

- non cliccare sui link contenuti nel messaggio sospetto
- controllare periodicamente lo stato del proprio conto online, nel caso in cui se ne possieda uno
- controllare la sicurezza del sito che stiamo visitando. Prima di inviare eventuali informazioni personali, assicurarsi che la URL relativa al sito, presenti caratteristiche di protezione adeguate
- controllare che l'indirizzo web nella barra del browser sia corrispondente a quello a noi noto e, quando si accede a un servizio in modalità sicura, verificare che l'idirizzo abbia la dicitura iniziale "https://" anzichè "http://"
- controllare che nella barra di stato del browser, nel momento in cui visitiamo una pagina che utilizza una connessione sicura crittografata, sia presente l'icona che indica tale stato di protezione
- installare sul proprio pc un software antivirus o altri software antispam. Questo è importante anche per contrastare le minacce provenienti dai messaggi di phishing.

Comunità virtuali

COSA È UNA COMUNITÀ VIRTUALE

Nelle comunità di tipo tradizionale, l'appartenenza di un membro non dipende esclusivamente dalla sua volontà le persone sono unite da rapporti sociali, linguistici e morali, vincoli organizzativi, interessi e consuetudini comuni. In questo tipo di realtà vi è grande fiducia del gruppo nel gruppo e raramente l'appartenenza viene messa in discussione.

Le comunità virtuali (o Virtual Communities) rappresentano una nuova forma di aggregazione, sviluppatasi con l'avvento delle reti telematiche. Esse sono dei luoghi "virtuali", in cui gruppi di utenti, uniti da interessi e bisogni comuni, si incontrano e dialogano in tempo reale, superando qualsiasi barriera geografica.

A differenza delle comunità di tipo tradizionali e quelle virtuali, sono molto più dinamiche ed in continua evoluzione; in queste comunità l'appartenenza deriva esclusivamnte da un'adesione esplicita dell'individuo.

All'interno delle comunità virtuali vengono simulati dei veri e propri spazi sociali, luoghi di incontro fisico o virtuale, all'interno dei quali vengono prodotte, diffuse e scambiate conoscenze e informazioni.

L'interazione, in questo tipo di contesto, si basa solo su ciò che gli utenti scrivono, annullando le differenze nella

gerarchia sociale e organizzativa.

Caratteristiche come classe, razza, genere, età, modo di vestire, assumono un aspetto ininfluente ai fini dell'interazione, che per questo si rivela unica e altamente "democratica".

COME FUNZIONA UNA COMUNITÀ VIRTUALE

Le comunità virtuali sono fondate su un patto ed uno scambio comunicativo. Chi vi accede accetta di entrare in contatto con le informazioni altrui, ma deve anche accettare il principio per cui lui stesso deve condividere informazioni proprie. Affinché una comunità raccolga i consensi degli utenti, è necessario che sia caratterizzata da elementi distintivi, ovvero argomenti specifici che attraggano gli stessi.

L'utilizzo delle comunità virtuali prevede, come presupposto, la conoscenza di una sorta di galateo virtuale, che per alcuni aspetti è abbastanza intuitivo, per altri potrebbe risultare incomprensibile a persone che non abbiano utilizzato a lungo questa forma di comunicazione. Infatti molte regole, che gli utenti abituali considerano implicite, sono collegate alle caratteristiche tecniche del mezzo informatico. È comunque buona norma prendere visione degli specifici regolamenti prima di entrare a far parte di una comunità.

Per spingere gli utenti a comportarsi nel pieno rispetto delle regole, in molti forum, mailing-list e chat (e, a volte, anche news-server) viene richiesta la registrazione tramite

l'acquisizione di un nickname (soprannome unico), destinato a fornire un'identità all'utente, ed una password, necessaria per accedere al servizio.

In questo modo ogni utente registrato, definendo un profilo personale, possiede una propria identità necessaria per essere "riconosciuto" e contattato dagli altri.

Un profilo può essere ulteriormente corredato da altre informazioni, quali l'indirizzo di posta elettronica, un' immagine personale associata al proprio nickname, ed eventuali dati personali che si intende rendere visibili (per esempio dati riguardanti i propri gusti e abitudini).

I siti che ospitano comunità virtuali cercano di mettere a disposizione dei propri iscritti numerosi strumenti gratuiti, utili per comunicare: offrono spazio web per creare le proprie pagine personali, danno la possibilità di inviare cartoline elettroniche, dedicano pagine a oroscopo, SMS gratuiti, screen saver, hard disk virtuale online e quant'altro necessario per attirare attenzione ed interesse.

Esistono diversi tipi di comunità virtuali, classificabili in base alle esigenze dei membri che ne fanno parte e al target a cui si rivolgono. Esistono comunità strutturate, comunità non strutturate e comunità a struttura mista. Nelle comunità strutturate si trovano leggi e sanzioni autoimposte, sistemi formali per interagire, senso di appartenenza al gruppo ed un alto livello di coinvolgimento; a loro volta queste comunità possono essere aperte, se danno la possibilità a chiunque di entrarvi.

Nelle comunità virtuali non strutturate non vi è alcuna restrizione all'accesso; vengono generalmente costituite in breve tempo e vi è un'interazione molto veloce. Spesso

vengono aperte al momento dell'entrata dell'utente e chiuse quando non ci sono più persone online. Le comunità a struttura mista, infine, sono caratterizzate da un'identità abbastanza stabile, una barriera alla partecipazione ma non all'ingresso, una modalità di comunicazione completamente asincrona, semplicità nell'accesso con una velocità intermedia ed una facilità di uscita dal gruppo.

PRINCIPALI MINACCE

Le comunità virtuali, come servizio di comunicazione, non presentano particolari rischi da un punto di vista tecnologico; le maggiori minacce possono provenire da falle di sicurezza informatica o più in generale dalla cosiddetta tecnica di "ingegneria sociale" (studio del comportamento individuale di una persona al fine di carpire informazioni). Un malfunzionamento del servizio o principalmente l'inesperienza degli utenti, comportano problemi non solo per l'utente coinvolto, ma spesso anche per i suoi contatti. Infatti i truffatori, nascosti dietro eventuali bug, possono prendere il controllo del PC dell'utente e accedendo all'interno del suo sistema, rintracciare dati personali ed altre informazioni sensibili.

A volte anche la stessa ingenuità delle persone può rendere una comunità virtuale fonte di pericolo, ad esempio se si accettano file da sconosciuti che potrebbero nascondere virus, oppure si scambiano le proprie informazioni con sconosciuti apparentemente amichevoli, ma che hanno intenzioni non del tutto oneste. Grazie alla loro facilità d'uso, basta infatti una semplice registrazione "anonima"

per entrare nell'area di discussione.

Gli strumenti di comunicazione online quali le chat, i blog, i forum, ecc. nascondono diversi tipi di pericoli, soprattutto nei confronti degli adolescenti. A tal proposito vanno annoverati l'adescamento ed il bullismo.

Quando i minori accedono all'interno di queste comunità virtuali, possono entrare in contatto con persone sconosciute, intrattenere discussioni poco adatte alla loro età e, a volte, essere oggetto di attacchi verbali che possono avere un effetto offensivo o intimidatorio nei loro confronti.

Uno dei rischi in cui possono incorrere i ragazzi utilizzando chat, forum e blog è quello di interagire con i cosiddetti adescatori online.

I ragazzi rappresentano la fascia di utenti più vulnerabile agli attacchi degli adescatori.

L'anonimato offerto dalla rete consente di instaurare rapidamente relazioni con i minori; gli adescatori tentano di attrarre le loro vittime offrendo attenzioni, gentilezze e dimostrandosi interessati ai loro problemi.

Riescono in poco tempo a conoscere hobby, gusti e preferenze delle loro vittime e tentano di avere approcci con loro. A volte, per tentare di allentare le inibizioni dei giovani, introducono nella conversazione argomenti a sfondo sessuale o materiale che mostra esplicitamente scene di sesso. Molti adolescenti cercano di affrontare e risolvere i propri problemi rivolgendosi ad esempio a forum di supporto, ed è proprio qui che gli adescatori aspettano le loro vittime.

Alcuni lo fanno in modo graduale, inizialmente

mostrandosi particolarmente interessati a risolvere i problemi, offrendo loro particolare riguardo e, a volte, anche dei regali. Altri invece agiscono in modo meno graduale avviando immediatamente conversazioni che trattano apertamente di sesso.

È proprio in età adolescenziale che si inizia ad esplorare la propria sessualità, cercando di sfuggire al controllo degli adulti e andando alla ricerca di nuove relazioni al di fuori del nucleo familiare. Ragazzi che nella vita reale restano lontani da comportamenti azzardati, quando sono online si mostrano più propensi a correre dei rischi grazie alla protezione che l'anonimato offre loro.

Il bullismo o cyber-bullismo invece, è un'aggressione sociale online che può manifestarsi in svariate forme: inviare sms o e-mail intimidatorie con insulti e pesanti offese, lasciare sui blog commenti offensivi con l'intento di danneggiare o rovinare la reputazione di qualcuno, accanirsi contro una persona con messaggi elettronici ripetuti.

In sostanza, il bullismo come comportamento offensivo è diretto verso una vittima particolare, incapace di difendersi perché giovane, debole o psicologicamente insicura.

Le caratteristiche di un atteggiamento da bullo possono essere:

- aggressività generalizzata
- impulsività e irrequietezza
- scarsa empatia

- atteggiamento positivo verso la violenza
- disimpegno morale
- autostima medio-alta
- oppositività ed aggressività verso gli adulti
- forte senso di indipendenza

COME DIFENDERSI

Il dinamismo e la tipologia dei mezzi di comunicazione utilizzati nelle comunità virtuali, se da un lato apportano numerosi vantaggi volti all'innovazione e alla diffusione delle competenze tecnologiche, dall'altro comportano alcune limitazioni.

La mancanza di interazione fisica ed il continuo cambiamento del gruppo causano delle difficoltà nella costruzione della fiducia, elemento fondamentale nell'ambito della comunicazione.

Nell'utilizzo delle comunità virtuali è buona norma adottare comportamenti responsabili al fine di evitare di imbattersi in situazioni poco gradevoli.

È opportuno non utilizzare i servizi offerti dalle comunità virtuali per comunicare dati sensibili o personali: ad esempio la password della propria e-mail, o il numero della propria carta di credito. Infatti i dati scambiati attraverso questi servizi che, sono del tutto trasparenti che potrebbero quindi essere "intercettati" da utenti estranei per secondi fini.

Non accettare nei propri contatti personali utenti estranei e non distribuire in modo incontrollato il proprio indirizzo e-mail.

I malintenzionati potrebbero sfruttare questi canali di comunicazione per intraprendere un tipico attacco informatico.

Qualora il servizio prevedesse lo scambio di file, è opportuno accettare solo file provenienti da persone conosciute e fidate: il servizio potrebbe essere sfruttato per l'invio di file apparentemente innocui, ma che contengono virus o altri tipi di malware.

Se non si è certi della provenienza, è bene non prendere in considerazione link inviati da altri utenti, poiché aprendoli si potrebbe essere reindirizzati su siti non legittimi.

È fondamentale inoltre installare un software Antivirus sul proprio PC, in grado di operare in real-time, filtrando eventuali file infetti. Se è prevista la condivisione di file e si vuole condividere qualche documento del proprio sistema, è opportuno porre molta attenzione alla configurazione del client che fornisce il servizio, per evitare di esporre involontariamente contenuti ritenuti confidenziali.

Per evitare di essere vittime del bullismo, si possono adottare le seguenti precauzioni.

Innanzitutto è bene conoscere il fneomeno e sapere di cosa si sta parlando; dare il giusto valore ai comportamenti prepotenti ricorrendo, se necessario, ad indagini per rivelarne la diffusione e portare allo scoperto comportamenti nascosti; creare un clima sicuro in cui si possa stimolare i ragazzi a raccontare all'adulto ciò che accade; fare chiarezza sui fatti e combattere insieme il

fenomeno; intervenire nei singoli episodi in modo da fermare l'aggressione e cercare, in un secondo momento, di capire cosa è successo, quali sono i fattori e le cause scatenanti; supportare le vittime.

È opportuno, infine, ricordare che, in ogni situazione di bullismo, la vittima è la persona che ha più bisogno di aiuto immediato; spesso a subire violenza da parte di coetanei sono ragazzi isolati, con pochi amici, introversi.

Acquisti online

COSA SONO GLI ACQUISTI ONLINE

Quando si parla di acquisti online si fa riferimento al termine "commercio elettronico" o "e-commerce", che indica espressamente l'atto di acquisto o di vendita di beni o servizi svolto mediante il computer.

In generale, il commercio elettronico può essere definito come una qualsiasi transazione effettuata per la vendita o l'acquisto di un prodotto o di un servizio, in cui i protagonisti interagiscono elettronicamente piuttosto che con scambi fisici e contatti diretti.

L'inizio del commercio elettronico risale agli anni '70, quando attraverso l'utilizzo di reti private, le aziende potevano scambiarsi informazioni di tipo commerciale, in modo tale che fornitori ed acquirenti comunicavano tra loro aggiornandosi costantemente. Questo imponeva dei limiti sia sul formato dei documenti scambiati attraverso la rete privata, sia per l'accesso al servizio. Solo il personale interno all'azienda era in grado di usufruire di tale servizio, mentre gli esterni, non possedendo le dovute autorizzazioni, erano esclusi.

Con l'avvento di Internet si è passati ad un vero e proprio mercato globale, senza limiti geografici e soprattutto senza limiti di utilizzo, in cui i siti web si trasformano in negozi

virtuali dai quali acquistare ogni genere di prodotto.

Il produttore ha la possibilità di diffondere il proprio messaggio elettronicamente, modificandolo ed aggiornandolo in tempo reale; ha inoltre la possibilità di interagire direttamente con il consumatore e permettere alle aziende che vi ricorrono, di essere più competitive sul mercato. Generalmente quando si acquista sul web, la fase preliminare di ordine e l'eventuale pagamento vengono effettuati online, ma il bene richiesto viene poi spedito a domicilio o alla sede dell'acquirente.

Il commercio elettronico presenta caratteristiche diverse a seconda dei soggetti che ne prendono parte: cittadino, imprese, istituzioni. In particolare, se il protagonista è il consumatore generico, esistono due diverse modalità:

- la "business to consumer" (da azienda a consumatore) prevede un azienda che offre i propri prodotti al consumatore finale, il quale decide se acquistarli e con quale forma di pagamento
- la "consumer to consumer" (da consumatore a consumatore) in cui gli utenti nella rete scambiano tra loro prodotti. Quest'ultima forma di commercio si è sviluppata grazie alla forte espansione dei siti di asta online, come ad esempio eBay.

COME FUNZIONANO GLI ACQUISTI ONLINE

L'acquisto online può avvenire in due diverse modalità a seconda del bene o servizio che si intende acquistare: modalità "diretta" e modalità "indiretta".

Un acquisto online si definisce diretto se tutte le fasi della transazione avvengono online, ovvero sia l'ordine, sia il pagamento e la consegna avvengono elettronicamente. Fanno parte di questa categoria tutti i beni digitali (quali software, dischi, canzoni o filmati in formato digitale) e tutti i servizi la cui fruizione avviene attraverso Internet (servizi di biglietteria, scommesse, giochi online, banking), trasmissibili attraverso la rete.

Un acquisto online si definisce invece indiretto se la fase preliminare di ordine ed eventualmente anche il pagamento avvengono online, ma il bene viene recapitato fisicamente al domicilio o alla sede dell'acquirente. Si tratta di beni tradizionali (come computer, accessori, libri,…), in cui il venditore sfrutta la forma elettronica per espandere i canali di vendita ed incrementare il numero dei clienti. In questo caso verificare il buon esito di una transazione è molto più semplice, dal momento che la mancata ricezione del bene mostra chiaramente un malfunzionamento.

Nel caso di un acquisto diretto, ciò risulta più difficile; l'unico indizio è l'avvenuto pagamento tra le parti, ma spesso ottenere le prove dei trasferimenti finanziari non risulta semplicissimo.

Il venditore deve attrezzarsi per:

- rispondere tempestivamente a qualunque richiesta di chiarimenti o di assistenza da parte degli utenti
- evadere gli ordini nei modi e nei tempi precisati nel sito web
- tenere costantemente aggiornati i cataloghi e tutti i contenuti del sito.

Per poter effettuare un acquisto online è necessario seguire un iter preciso all'interno del sito preposto al commercio elettronico. L'acquirente deve per prima cosa visitare il negozio virtuale (www.negoziovirtuale.it) per decidere se acquistare o meno i prodotti a disposizione.

Generalmente per ciascun prodotto è prevista una scheda informativa completa di prezzi, immagini, caratteristiche tecniche, in modo da fornire all'utente più informazioni possibile. Dopo aver selezionato i prodotti di interesse, l'acquirente passa alla compilazione di un form, in cui vengono richiesti tutti i dati necessari (nome, cognome, indirizzo,...) affinché il negozio virtuale recapiti correttamente l'ordine.

È il momento di recarsi alla cassa: qui bisogna decidere la modalità di pagamento desiderata. Tra le più comuni troviamo:

- bonifico bancario
- carta di credito
- pagamenti online
- contrassegno.

Il bonifico bancario deve essere anticipato, ovvero una volta effettuato l'ordine, viene spedita la mail all'acquirente contenente i dati dell'ordine e gli estremi del conto corrente sul quale effettuare il bonifico.

Con questi dati basta effettuare il pagamento allo sportello bancario oppure, per chi possiede un conto corrente online, comodamente davanti al proprio pc. Occorre poi inviare gli estremi del pagamento al venditore, che verifica il trasferimento fondi e provvede alla spedizione del prodotto.

Esistono diverse modalità di pagamento via elettronica, tra cui:

- carta di credito
- carte di credito ricaricabili (come la Poste Pay); entrambe richiedono un codice segreto per essere utilizzate.

Le carte di credito ricaricabili hanno un costo di attivazione e possono poi essere usate a proprio piacere depositandovi sopra la somma di denaro voluta. Una volta finita la disponibilità la carta si blocca finché non vi vengono depositati altri soldi.

A differenza del bonifico bancario, il pagamento tramite carta di credito non ha costi aggiuntivi oltre a quelli previsti per gli acquisti effettuati.

Infine, alcuni venditori accettano il contrassegno, che viene però corredato delle spese accessorie di riscossione.

PRINCIPALI MINACCE

Gli acquisti online offrono numerosi vantaggi sia per il venditore che per i consumatori.

Le aziende che sfruttano il canale del commercio elettronico hanno la possibilità di entrare in contatto con i clienti finali senza alcuna intermediazione, riuscendo ad offrire un trattamento personalizzato. Molti siti e-commerce invitano i clienti ad indicare le proprie preferenze e i propri

interessi, da qui ne scaturisce una sorta di "profilo" dell'utente di cui servirsi per offerte commerciali.
Uno dei vantaggi più rilevanti risiede nel fatto che studiando gli acquisti effettuati online dai clienti, ed analizzando le pagine più consultate della categoria, il venditore può ricevere un feedback in tempo reale dal mercato, riscontrando personalmente l'impatto che un nuovo prodotto ha avuto sulla clientela.

Per i consumatori che usufruiscono di tale servizio, invece, c'è sicuramente un'ampia offerta di prodotti e di servizi con la possibilità di personalizzarli; un notevole risparmio sul prezzo di acquisto unito ad una risposta rapida delle richieste e ad un'assistenza tempestiva; infine la possibilità di visionare prodotti e servizi 24 ore al giorno senza limitazioni geografiche.

Ci sono, però, alcuni svantaggi da tenere ben presente:

- la riservatezza e la tutela dei dati personali
- la sicurezza e la scarsa trasparenza delle transazioni finanziarie
- la sicurezza dei pagamenti elettronici
- la garanzia della qualità del prodotto.

Uno svantaggio dell'acquistare un prodotto tramite il computer risiede nel fatto di non poter toccare materialmente il prodotto, si compra senza aver avuto alcun contatto fisico con la merce, a meno che non lo si conosca per averlo già visto in qualche negozio reale. In secondo luogo troviamo problematiche relative alla merce difettosa; se la merce acquistata dovesse rivelarsi malfunzionante o non integra, o se semplicemente non risponde alle aspettative, è necessario contattare il venditore per far

presente il problema e rispedire indietro il prodotto. I costi della seconda spedizione sono a carico di chi acquista.

Un tasto dolente è rappresentato dai pagamenti in modalità elettronica.

Con il bonifico bancario non si corrono grandi rischi sia per il venditore che per l'acquirente, bisognerà però attendere qualche giorno prima che la merce acquistata venga spedita. Inconvenienti possono verificarsi nel caso di bonifici all'estero; le banche italiane caricano su questi trasferimenti spese altissime, in qualche caso spropositate, addirittura più elevate del costo previsto per l'acquisto della merce desiderata. Con la carta di credito, invece, non sono previsti costi aggiuntivi, ma esiste il problema di far viaggiare dati personali (relativi al numero del conto di credito) sulla rete. Anche se il venditore effettua correttamente la transazione, addebitando al cliente il giusto dovuto, conserverà memorizzati i vari numeri di conto; se questi dovessero essere espugnati da un hacker, ecco che la carta di credito cadrebbe in mani sbagliate.

COME DIFENDERSI

Acquistare online merce proveniente da qualsiasi parte del mondo, comodamente seduti davanti al proprio computer è sicuramente una prerogativa eccellente, che bisogna però saper sfruttare nel modo giusto onde evitare spiacevoli sorprese. La rete globale di Internet offre possibilità infinite in tutti i campi della vita quotidiana, compreso lo shopping.

Non tutti i prodotti commerciali si prestano bene per essere acquistati su Internet. Il primo fattore da valutare è il risparmio, bisogna cioè capire se, a conti fatti, comprare su Internet permette di risparmiare solo pochi spiccioli rispetto all'acquisto in un negozio reale o in un centro commerciale, oppure consente un notevole risparmio di denaro.

Al prezzo reale del prodotto, vanno sommate spese accessorie (imballo e spedizione) che dipendono dal peso e dalle dimensioni del pacco: più sarà grande e pesante l'oggetto acquistato, maggiori saranno le spese di trasporto. Per questo motivo, soprattutto per grandi distanze, per il commercio online è conveniente acquistare oggetti piccoli e di alto valore piuttosto che oggetti voluminosi, pesanti e di medio valore. In secondo luogo, qualora il prodotto desiderato lo preveda, è opportuno tener presente la garanzia e l'eventuale manutenzione. Ad esempio, nel caso di prodotti elettronici l'acquirente dovrebbe verificare se siano assistiti in zona con tutte le garanzie: è inutile acquistare in un paese lontano una merce elettronica se non fosse poi possibile ripararla in Italia.

Con i pagamenti elettronici, come descritto nelle sezioni precedenti, si possono subire delle vere e proprie truffe con conseguenze economiche anche gravi. Utilizzando la modalità bonifico bancario, è indispensabile verificare la località di destinazione di trasferimento, dal momento che per trasferimenti all'estero le banche italiane aggiungono somme di denaro consistenti. Con la carta di credito invece, esiste il rischio di far viaggiare i propri dati in rete; per non rinunciare ai privilegi di questa modalità di pagamento

sono nate carte di credito ricaricabili. Sono sicure e anche relativamente comode, ma devono essere tenute sotto controllo per evitare che ci siano troppi soldi quando non servono e, viceversa, che ci sia la somma necessaria per fare gli acquisti quando serve. In questo modo, qualora qualche malintenzionato sulla rete riuscisse a scoprire il codice segreto di tale carta, non troverebbe disponibilità di denaro da poter utilizzare per scopi illeciti. È quindi consigliabile utilizzare carte ricaricabili piuttosto che carte di credito.

Solitamente nei siti e-commerce è prevista un'apposita sezione che spiega le regole di pagamento, è opportuno leggerlo con attenzione. Non mandare mai soldi contanti in una busta o tramite raccomandata.

Oltre alle vere truffe, esistono spiacevoli sorprese che non sono necessariamente illegali, ma che arrecano comunque un notevole fastidio. Una delle principali è la spedizione, dipendente dal paese di origine e di destinazione, dal tipo di corriere e di spedizione scelti. Acquistare da paesi stranieri extra europei impone anche il pagamento del dazio doganale, che si aggira intorno ad un quarto del prezzo dell'oggetto; è bene verificare l'ammontare di questi costi prima dell'acquisto. Alcuni siti lo indicano con chiarezza, indice di serietà e professionalità, altri invece nascondono questa informazione, svelandola all'acquirente solo ad acquisto avvenuto.

Il grande difetto degli acquisti online risiede nell'impossibilità di constatare fisicamente la qualità del prodotto. C'è il rischio di una spiacevole sorpresa ricevendo un oggetto che non è quello che si supponeva. Nel caso di prodotti noti e di larga diffusione questi problemi non dovrebbero sussistere, se invece si hanno dei dubbi, ci si può sempre recare in un centro commerciale

per una valutazione fisica prima di procedere all'acquisto online.

Da non dimenticare un dritto importantissimo per l'acquirente. Per la legge italiana l'acquirente ha il diritto di recesso entro un termine ben preciso (a seconda degli stati arriva fino a 14 giorni, nel caso di acquisti online fa fede il timbro postale). Si può recedere se il prodotto non piace, non è quello che si pensava, o semplicemente si è cambiata idea. In tutti i casi è necessaria la rispedizione del prodotto, con costi a carico dell'acquirente. È necessario mantenere il codice di spedizione del pacco per eventuali reclami in caso di disputa.

Alla luce di tutto ciò, è consigliabile a chi opera acquisti online di verificare sempre le condizioni di acquisto dei beni e le informazioni sul venditore, questo permetterà di comprenderne la serietà e l'affidabilità.

P2P

COS'È IL P2P

"Peer to peer" o l'abbreviazione P2P, sta per "condivisione di risorse tra pari", dal significato di peer = pari, uguale.

È un sistema di condivisione di file basato su una nuova tecnologia che sta assumendo sempre più importanza nel campo dell'informatica.

Un sistema peer to peer è formato da diverse entità (peer), capaci di auto-organizzarsi e condividere un insieme di risorse distribuite presenti all'interno di una rete di computer.

Lo scopo di tale sistema è scambiare risorse all'interno di una comunità; ogni peer fornisce una risorsa e ne riceve in cambio altre.

L'esempio classico di P2P è la rete per la condivisione di file (file-sharing). La situazione più comune riguarda lo scambio di musica: si offre musica alla comunità e si riceve altra musica in cambio. Ciascun peer può decidere di offrire gratuitamente le risorse residenti sul proprio sistema, mettendole a disposizione a tutti gli altri peer.

Le risorse che si possono condividere sono:

- potenza di calcolo
- banda

- spazio di memorizzazione
- informazioni.

Con i sistemi peer to peer spuntano fuori aspetti fondamentali, come sicurezza, autenticità e integrità dei file, riservatezza ed anonimato.

COME FUNZIONA IL P2P

Generalmente quando si parla di servizi forniti da Internet si è soliti utilizzare vocaboli come client e server.

L'architettura Client/Server prevede l'esistenza di calcolatori denominati "server" ed altri "client"; lo scopo del server è quello di soddisfare le richieste provenienti da diversi client. In pratica, il server mette a disposizione un servizio a diverse entità client e ciascun client va a prelevare informazioni contenute nel server.

Dal momento che più client possono effettuare contemporaneamente l'accesso al server, quest'ultimo deve prevedere dei meccanismi necessari alla gestione di connessioni multiple.

Esempi di servizi su Internet che presentano tale tipologia di architettura sono il WWW, la posta elettronica, l'FTP (servizi basati sullo scambio di file). Questi sono sistemi fortemente centralizzati, in netto contrasto con la natura estremamente distribuita dei sistemi peer to peer. Mentre nel client/server alcuni computer sono dedicati a servirne altri, nel P2P tutti i computer sono paritari, ovvero funzionano sia come client che come server.

Le risorse condivise si trovano "ai bordi" di Internet,

vengono cioè fornite direttamente dai peer che interagiscono tra loro senza l'intervento di un server centralizzato, implementando un paradigma basato su una cooperazione decentralizzata.

I singoli nodi, quindi i singoli computer, sono collegati tra loro attraverso la rete Internet; non è presente un server centrale verso cui indirizzare le comunicazioni dei vari nodi che invece comunicano direttamente.

Ciascun peer si connette al sistema in modo intermittente: sono infatti molto frequenti disconnessioni e riconnessioni al sistema da parte di uno stesso utente. Le risorse offerte dai peer vengono aggiunte e tolte dinamicamente. Ad un peer può essere associato un indirizzo IP diverso ad ogni diversa connessione al sistema; per questo motivo è impossibile localizzare una risorsa mediante un indirizzo IP statico.

Per migliorare la performance del sistema sono possibili soluzioni ibride, in cui ad esempio è previsto un server centrale per la localizzazione delle risorse condivise. Nei sistemi P2P tradizionali passando attraverso la rete sono in grado di collegarsi direttamente agli altri peer (presenti in rete), ed utilizzando un'applicazione software, possono condividere file multimediali o documenti.

Ciascun computer (peer) è responsabile del passaggio dei dati agli altri computer, svolgendo allo stesso tempo compiti sia di client che di server.

Le funzioni importanti nel P2P sono:

- discovering, ovvero l'azione atta a scoprire gli altri peer
- queryng, ovvero la richiesta di contenuti ad altri peer
- sharing, ovvero la condivisione delle proprie risorse.

Come può, ad esempio, un utente riuscire ad ottenere un

file musicale da un altro utente?

Innanzitutto l'utente deve essere in possesso di un applicativo P2P sul proprio computer. Successivamente è necessario che egli si connetta ad Internet, ottenendo così un indirizzo IP (solitamente diverso ad ogni nuova connessione).

A questo punto può offrire alla comunità alcune canzoni (memorizzate nel proprio computer), registrandole in un'apposita directory condivisa; allo stesso tempo sottomette una query al sistema, specificando il titolo della canzone o l'artista cui è interessato.

L'applicativo P2P visualizza le informazioni circa gli altri peers che posseggono la canzone richiesta; in base a queste, l'utente seleziona un peer dal quale ottenere la canzone. Il file viene copiato dal computer dell'utente scelto a quello dell'utente che effettua la richiesta.

Nello stesso moment in cui un utente sta effettuando il download, mette a disposizione del sistema i suoi dati (musica. ecc.) per far si che altri utenti possano accedervi.

In particolare un software P2P permette di:

- definire una directory, nel proprio file system, dove memorizzare i file che si intende condividere con la comunità; ogni altro utente può reperire uno di quei file da quella precisa directory (il peer si comporta come un web server)
- consentire di copiare file dalle directory di altri utenti (il peer si comporta come un client)
- individuare il materiale desiderato mediante specifiche richieste al sistema (funzionalità analoga ai motori di ricerca).

Esistono diversi software per il servizio P2P, tra i più famosi

troviamo Kazaa, Emule, Gnutella, Morpheus, ma molti altri sono facilmente reperibili in rete, pronti da scaricare sul proprio computer.

PRINCIPALI MINACCE

Il peer to peer si è rivelato un enorme successo nell'ambito dell'informatica, testato dalla grande diffusione dei software peer to peer per il file-sharing. Purtroppo però, insieme ai notevoli vantaggi (elevata quantità di risorse a disposizione, veloce distribuzione delle informazioni da un peer ad un altro scavalcando qualsiasi filtro centrale), è importante conoscere le problematiche che si nascondono dietro questo sistema, soprattutto se utenti malintenzionati sfruttano il canale comunicativo peer to peer per diffondere nuovi virus in pochissimo tempo.

Innanzitutto non vi è garanzia che il contenuto dei diversi peers sia sempre disponibile; se un utente scollega il proprio computer dalla rete, tutte le risorse che possiede non sono più accessibili da parte di altri utenti. Essendo un sistema aperto, è facilmente attaccabile dagli hacker per la propagazione di qualsiasi tipo di dati, soprattutto malevoli.

Sono molti gli esempi di programmi per il file-sharing che contengono al loro interno spyware per studiare le preferenze degli utenti e adware per pubblicizzare particolari siti o prodotti di mercato.

Un attacco particolare alle reti peer to peer per il file-sharing è il cosiddetto poisoning. Esso consiste nel diffondere nella rete un file (generalmente contenente dati

dannosi per il computer, come ad esempio i virus) spacciandolo per un altro, allo scopo di ingannare utente che ne viene in contatto.

Un dubbio che potrebbe sorgere e che è importante chiarire, riguarda la legalità del P2P. Il peer to peer in sé, inteso come scambio e condivisione di file, non è illegale, ma un aspetto fondamentale da non trascurare è il fatto che esso favorisce la violazione dei diritti d'autore. Ciò che potrebbe rendere illegale un software file-sharing è l'illeicità dei contenuti condivisi dagli utenti.

Attraverso le reti P2P gli utenti possono condividere gratuitamente file di ogni genere (musica, film, programmi, immagini, testi), e facilmente si può incorrere nella violazione del copyright.

La legge sul "diritto d'autore" non tutela l'autore stesso ma la sua opera, purché abbia le seguenti caratteristiche:

- sia un'opera di ingegno (ovvero il risultato di una attività intellettuale creativa)
- abbia carattere creativo (deve essere non banale, originale ed innovativa)
- appartenga ad un determinato genere artistico (letteratura, musica, architettura, teatro e cinema)
- abbia espressione di concretezza (le idee non sono suscettibili di protezione finché non gli si dà concretezza).

È utile capire quali sono i file che possono essere scambiati senza alcuna conseguenza legale e quali no. Un software proprietario può essere utilizzato dall'utente finale solo se in possesso della licenza d'uso, rilasciata a seguito di pagamento. All'utente è consentito effettuare solo una copia di sicurezza, utile in caso di malfunzionamento del programma o smarrimento della copia originale.

La duplicazione abusiva di questo tipo di software è sanzionata penalmente, ed è evidente che chi trasmette tramite sistemi P2P un software proprietario abusivamente duplicato, commette reato.

Pareri discordanti ci sono invece per quel che riguarda il problema di scaricare copie non autorizzate; bisognerebbe valutare attentamente ogni singolo caso prima di dare un giudizio.

Quanto detto per il software proprietario non vale per il software freeware, che può essere utilizzato e copiato gratuitamente, né per lo shareware, software rilasciato in prova per un determinato periodo di tempo e che può essere utilizzato e copiato entro i termini previsti nella licenza.

Nell'ambito della condivisione dei file, vengono scaricate via Internet numerose opere protette dal diritto d'autore: il problema risiede nel fatto che mettere a disposizione di terzi un'opera protetta costituisce un'attività illegale se il titolare dei diritti non ha dato il suo assenso. Il crescente successo del file-sharing ha indotto i titolari di diritti d'autore e i loro rappresentanti a promuovere azioni legali per contrastare la pirateria digitale.

COME DIFENDERSI

Negli ultimi anni l'utilizzo del software P2P si è diffuso rapidamente, grazie alle connessioni sempre più veloci e alla sempre crescente capacità di compressione dei file, mantenendo inalterata la qualità degli stessi.

Con il P2P è aumentata anche la diffusione di file malware, che minacciano l'integrità e la sicurezza del nostro computer.

Per contrastare tale fenomeno è necessario adottare le dovute precauzioni. Innanzitutto è necessario imparare a conoscere il funzionamento del programma P2P che si utilizza, e in particolare impostare i parametri di configurazione con cui il programma andrà a condividere i file.

È consigliabile specificare manualmente i file e le cartelle da condividere, facendo attenzione a non selezionare cartelle o sottocartelle che contengono documenti importanti o privati. Generalmente tutti i file che vengono acquisiti tramite il sistema P2P, vengono salvati all'interno di un'unica cartella (denominata "File condivisi").

È sempre utile controllare la natura di questi file per evitare eventuali complicazioni, ad esempio assicurarsi di non aver infranto il copyright.

Di recente è stato stabilito che l'uso del software P2P è legale ma solo se, quando lo si utilizza, si distingue fra materiale di dominio pubblico e materiale protetto da copyright. In caso di dubbi riguardo uno specifico file, è consigliabile non condividerlo o non scaricarlo.

Dimostrare la consapevolezza dell'utente finale di condividere software che violi il diritto d'autore non è cosa del tutto semplice, e questo ai fini sia penali che civili. Il grado di consapevolezza dell'utente sale in funzione della

sua esperienza, ma non sempre è facile conoscere in anticipo il contenuto e le caratteristiche del software che si scarica in rete. Così quando un utente scarica il file denominato "xyz.exe" si può ipotizzare che non ne conosca i contenuti fintanto che il file non sia stato completamente scaricato.

Del resto, una volta installato e valutato che il programma è di tipo "proprietario", è consigliabile cancellarlo dal computer, al fine di evitare problemi con le forze dell'ordine. Nell'utilizzo di sistemi P2P, oltre a considerare possibili rischi riguardanti la legalità delle opere condivise, è bene soffermarsi anche sulla sicurezza del nostro computer e sulla riservatezza dei dati memorizzati (dal momento che consentiamo al mondo intero di scaricare file dal nostro computer).

Per evitare di essere infettati dai virus contenuti nei file provenienti dalla rete è sufficiente osservare le normali regole per proteggersi dai virus.

Gli spyware e gli adware possono essere eliminati utilizzando appositi software diffusi in Internet, oppure possono essere evitati del tutto utilizzando del software garantito, ovvero proveniente da fonti affidabili.

Regola basilare è quella di munirsi di antivirus e set di programmi per la rimozione dello spyware prima di avventurarsi nel download del software. Non è possibile stabilire l'identità di ogni file presente sulle reti P2P, per cui non si può mai avere la certezza che un particolare file che si vuole scaricare non contenga malware.

Inoltre, un classico programma P2P garantisce un grado di anonimato pari a zero; tutti i peer con cui entreremo in contatto conosceranno il nostro indirizzo IP e quindi, potenzialmente, potrebbero attaccarci.

Diventa allora indispensabile la presenza di un buon firewall. In sostanza, occorre prestare molta attenzione nella selezione di software da scaricare ed adottare tutte le contromisure possibili per evitare di imbattersi in situazioni compromettenti per la sicurezza del proprio computer.