Il Sole 24 ORE.com

11 giugno 2009

Ladri di identità, hackers e spammers: come difendersi davanti al pc

La sicurezza informatica passa anche dalla consapevolezza dei propri diritti e doveri quando ci si muove nella rete. Alcune regole precauzionali potrebbero, invece, aiutare ad evitare di incorrere nei cyber criminali, sempre più diffusi nel web.

Diffamazione a mezzo internet
Le offese divulgate nella rete a più persone configurano il reato di diffamazione aggravata dal mezzo di pubblicità: le pene vanno dalla reclusione da 6 mesi a tre anni o della multa non inferiore a 516 euro. Il reato è integrato anche attraverso i social network o l'invio di messaggi diffamatori a mezzo e-mail. In generale, l'inserimento di frasi offensive, battute pesanti, notizie riservate la cui divulgazione provoca pregiudizi, ma anche foto denigratorie, la cui pubblicazione ha ripercussioni negative, anche potenziali, sulla reputazione della persona ritratta possono integrare gli estremi del reato di diffamazione. Inoltre, il consenso ad essere ritratti non comporta il consenso a utilizzare le foto, soprattutto se tale utilizzo avviene in contesti che espongono il soggetto a lesioni della propria reputazione. Il limite è sempre la continenza: non si possono utilizzare espressioni dotate di alta carica offensiva.

Il delitto di accesso abusivo ad un sistema informatico
E' punito con la reclusione fino a tre anni e sanziona la condotta di chi si introduce o si mantiene in un sistema informatico o telematico, protetto da misure di sicurezza, contro la volontà (espressa o tacita) di chi ha il diritto di escluderlo. La disposizione ha introdotto per la prima volta il bene giuridico del domicilio informatico, inteso come spazio ideale (ma anche fisico), di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale. Il cyberspazio, l'ambiente virtuale in cui l'individuo opera con le tecnologie informatiche, è assimilato allo spazio domestico fisico, purché dotato di quelle misure di sicurezza, come una semplice password di accesso, che manifestino la volontà del titolare di esercitare il proprio diritto di escludere terzi estranei.

Spamming
Lo spamming è quella condotta che si manifesta attraverso l'invio di mail o sms non richiesti dall'utente. Dal punto di vista civilistico, tale condotta configura un danno risarcibile di tipo non patrimoniale, che consiste in quei fastidi, stress, ansie, perdite di tempo, mancanza di serenità che turbano sfera esistenziale della vittima. Dal punto di vista penale, la condotta potrebbe configurare anche il reato di molestie. Secondo il Garante della privacy la condotta potrebbe risultare illecita sotto il profilo del trattamento dei dati della privacy.

Phishing
Consiste nella condotta di chi, inviando messaggi di posta elettronica o sms, contenenti il link di indirizzamento alla pagina web non autentica, induce l'utente o fruitore di un servizio on line a rivelare informazioni personali di carattere riservato che poi verranno utilizzate per accedere abusivamente ai servizi on line o ad aree riservate, o per utilizzare indebitamente carte di credito o di pagamento, realizzando un profitto. Di recente i phisher utilizzano sempre più spesso i telefoni cellulari per integrare il proprio disegno criminoso. In particolare, l'utente riceve un sms nel quale, per problemi connessi a presunte transazioni, viene invitato a contattare il numero telefonico della filiale della banca della propria città. A tale numero, che in genere è un numero in Voip, risponde una voce registrata che invita l'utente a fornire tutti i dati relativi alla carta di credito, al fine di effettuare delle presunte verifiche. In realtà, i dati vengono registrati e successivamente adoperati fraudolentemente dal phisher. In questi casi, all'autore possono essere contestati anche i reati di indebito utilizzo di carta di credito ex art. 12 d.l. 143/91, punito con la reclusione da uno a cinque anni, e la sostituzione di persona punita a sua volta con la reclusione fino a un anno. Nel caso dell' home banking, è configurabile anche il reato di detenzione abusiva di codici di accesso ad un sistema informatico o telematico, punito con la reclusione fino a un anno.

Frode informatica
Il reato di frode informatica è punito con la reclusione da sei mesi a tre anni e con la multa fino a 1.032 euro e in genere consiste nel penetrare attraverso un pc all'interno di server per clonare account di ignari utilizzatori del servizio o per usufruire gratuitamente di servizi a pagamento. Recentemente le frodi informatiche si sono realizzate anche con l'utilizzo del POS, un apparato elettronico di trasmissione dati, che consente di leggere, memorizzare e trasmettere i dati delle carte di credito (e dei titolari) contenute nella banda magnetica. I furti dei codici personali possono avvenire tramite microchip inseriti nei pos di supermercati, alberghi e negozi in generale.
Il reato può configurarsi anche attraverso le aste on line legate all'e-commerce (e-bay, ecc…). Le transazioni possono essere intercettate dagli autori delle frodi ed essere deviate su conti correnti diversi da quelli dell'originario venditore. In questi casi è possibile tutelarsi usando carte prepagate con importi contenuti e comunque utilizzando

sempre metodi di pagamento di cui esiste la prova perché tracciabili.
Le aste on-line possono esporre gli acquirenti anche ai rischi dei reati di ricettazione e incauto acquisto. Se non si è sicuri dell'origine della merce, meglio non effettuare la transazione. Potrebbe essere materiale contraffatto: anche chi acquista rischia un processo penale.
Anche la cosiddetta truffa dei numeri dialer può integrare il reato di frode informatica. In questi casi, in genere, accade che durante la navigazione internet, sul computer dell'utente viene scaricato un software non richiesto, che sostituisce il normale numero del provider di connessione in rete con un altro numero, cosiddetto dialer, dai costi di connessione elevatissimi. Spesso inoltre il dialer si sostituisce alla connessione predefinita, in modo da essere utilizzato inconsapevolmente dall'utente ad ogni collegamento.
La maggior parte dei dialers si trovano nei siti web che propongono loghi, suonerie, sfondi e trucchi per playstation, siti web per adulti, nonché siti che invitano a scaricare gratuitamente software, musica Mp3 e guide elettroniche.
I siti web che propongono dialers hanno l'obbligo di comunicare che la connessione è a pagamento, ma non sempre tale informazione arriva all'utente. Per difendersi da questi attacchi occorre fare attenzione ai file che si scaricano: se cliccando su uno dei links presenti nel sito viene chiesto di scaricare un file con estensione "exe" che offre loghi, suonerie ed altro, molto probabilmente si tratta di un dialer. L'unico rimedio consiste nell'uscire immediatamente dal sito e chiudere o annullare l'eventuale finestra che potrebbe aprirsi ancora sul desktop. I casi di dialer possono essere denunciati sia all'autorità Antitrust che alla polizia postale, al fine di ottenere anche la restituzione dell'indebito importo eventualmente pagato.

Pornografia minorile telematica
La detenzione di materiale pornografico minorile può dar luogo a pene che arrivano fino a tre anni di reclusione. Ma anche in questi casi è necessario prestare la massima attenzione: è possibile essere indagati per questo reato anche se si è completamente ignari di detenere materiale pedpopornografico sul proprio pc. Ovviamente si tratta di casi che dovrebbero restare marginali, ma il download inconsapevole di materiale illecito può verificarsi con varie modalità. Nel caso dei fruitori di peer-to-peer (e-mule, napster, ecc..) il rischio di scaricare inavvertitamente file illeciti può essere alto. Questo sistema di file sharing si presta alla condivisione, alla trasmissione e alla diffusione di qualunque tipo di file, sia audio che video, in assoluto anonimato. Può accadere che l'utente, credendo di scaricare file musicali o video, si trovi inavvertitamente sul pc materiale pedopornografico. Nel caso in cu, tale scambio dovesse essere intercettato, sarà però una buona consulenza tecnica o peritale a far luce sul livello di consapevolezza dell'utente, determinando spesso l'esito del procedimento penale. Determinanti, al fine della corretta valutazione della consapevolezza della condotta dell'utente, sono sia il suo grado di conoscenza di internet, che la cartella in cui vengono salvati i file. Se si tratta di una cartella temporanea (c.d. cache) presente su tutti i computer che adoperano sistemi operativi Window, sarà più agevole escludere la volontà del soggetto agente e quindi la sussistenza del reato.
Lo scambio di materiale pedopornografico, invece, è punito con la reclusione da sei a dodici anni e la multa fino a 258.228 euro. Casi frequenti di scambio di materiale illecito possono integrarsi tramite le chat (skype, messenger) o file allegati di posta elettronica. Soltanto nei casi in cui effettivamente l'utente avesse scaricato i file per sbaglio, sarà possibile dimostrarlo, con l'ausilio dei tecnici. In questi casi valgono le considerazioni precedenti.

File sharing
Per contrastare il fenomeno della condivisione di file attraverso la rete, il legislatore ha progressivamente introdotto nuove fattispecie di reato. Attualmente, la normativa distingue tra chi utilizza i programmi di file sharig (come e-mule) per fini di lucro e chi, invece, ne fa un uso privato. Nel primo caso è prevista una sanzione più severa, nel secondo una sanzione più blanda ed il reato può essere estinto con un meccanismo simile all'oblazione.

I consigli degli esperti

Professor Avvocato Lorenzo Picotti, Ordinario di diritto penale e diritto penale dell'informatica, Facoltà di Giurisprudenza di Verona

"Si possono distinguere due piani di difesa contro i crimini informatici: quello tecnico – organizzativo e quello culturale. Sotto il primo profil, è senz'altro necessaria, nell'epoca di Internet, l'adozione e l'aggiornamento costante di "misure di sicurezza" informatiche idonee, quali programmi antivirus, anti spamming, anti spyware o anti malware in genere, firewall, procedure di scansione periodica dei sistemi, ecc. Misure che sono obbligatorie, anche a pena di sanzioni penali, per chi tratta dati personali, secondo e gli standards previsti dal Codice della privacy (vedasi www.garanteprivacy.it).
Il mercato fornisce un'enorme gamma di prodotti, molti anche liberamente e gratuitamente accessibili in rete, che però bisogna evidentemente conoscere e controllare nelle loro caratteristiche, prima dell'installazione e dell'aggiornamento periodico. Su un diverso piano, è altrettanto e forse ancor più importante, strategicamente, promuovere una "cultura della sicurezza" anche attraverso "protocolli", disciplinari, codici etici ecc., in particolare nell'ambito di organizzazioni e strutture anche semplici, oltre che complesse, sia pubbliche che private, che vanno dalle aziende, specie bancarie, assicurative, finanziarie in genere, alle pubbliche amministrazioni, comprese scuole, Università, ospedali, servizi di ogni natura che sia avvalgono di risorse informatiche, quali associazioni, studi professionali, ecc…
Il nucleo essenziale di molti attacchi, in particolare di frodi, furti di identità, phishing soprattutto, che oggi tanto preoccupa, è costituito da tecniche di "social engineering", che sfruttano cioè l'"ingenuità", l'ignoranza, la pigrizia, le

cattive abitudini degli utenti, ossia il "fattore umano". In ultima analisi, e' proprio l'utente che – talora indotto maliziosamente in errore, come nel phishing, talora semplicemente "distratto" o negligente - fornisce credenziali di autenticazione per l'accesso ad aree informatiche riservate, od offre comunque occasioni di accesso illecito od appropriazione di dati ed informazioni, lascia aperte opportunità per intercettazioni o danneggiamenti, ai propri sistemi od anche al loro utilizzo per attacchi ad altri. E' importante sottolineare, poi, che si può essere inizialmente coinvolti in indagini su delitti informatici, per condotte od omissioni "non volute", da cui non è sempre facile o rapido essere scagionati.

Ad es., una delle forme più comuni di attacco informatico è quella c.d. man in the middle attack (MITM o MIM), nel quale l'attaccante è in grado di frapporsi fra due o più utenti, leggere, inserire o modificare a piacere, messaggi senza che nessuno degli utenti stessi sia in grado di sapere se il collegamento sia stato compromesso o "falsificato". Per cui possono essere "imputate" trasmissioni di materiali illeciti, comunicazioni costituenti reato, ecc. C'è anche il c.d. IP spoofing tramite la quale si crea un pacchetto IP nel quale viene falsificato l'indirizzo IP del mittente.

Possono aggiungersi gli accessi abusivi a sistemi (tramite diverse tecniche) che possono essere utilizzati per effettuare l'attacco ad altri sistemi.

Da queste tecniche devono distinguersi, invece, le condotte di mera visualizzazione di singole "pagine" web, quando l'utente accede ad es. anche casualmente a determinati siti (ad esempio pagine contenenti immagini pedopornografiche, od opere protette dal diritto d'autore). In questi casi, la giurisprudenza ha chiarito che la semplice "visualizzazione" di immagini pedopornografiche, senza che ne segua il down load, non configura la condotta (in sé altrimenti punibile) di "detenzione" od acquisto di detto materiale.

Lo stesso deve valere per ipotizzabili violazioni del diritto d'autore, che comunque, in difetto dell'elemento soggettivo del dolo (intenzionalità e comunque consapevolezza del fatto), non configurano un reato, ma al più un illecito amministrativo".

Avvocato Sandro Guerra, esperto di crimini informatici del foro di Firenze

"Non è difficile difendersi adottando banalissime cautele – spiega l'avvocato Sandro Guerra, esperto di crimini informatici - per esempio, prima di riempire un form o di comunicare il numero di carta di credito, suggerirei di chiedersi: darei questi dati ad uno sconosciuto interlocutore telefonico? Per quanto riguarda l'e-commerce, senza dubbio utilissimo per molti tipi di transazioni, in molti ignorano che in base ad una direttiva europea recepita dall'Italia nell'anno 2003 i siti che svolgono l'attività di commercio on line, o altro servizio della società dell'informazione, devono riportare una serie di informazioni obbligatorie, tra le quali la partita iva e i dettagli relativi all'iscrizione al registro delle imprese. Ma, probabilmente non vi è norma più violata di questa".

Domenico Vulpiani, Direttore del servizio di Polizia postale e delle Comunicazioni

"I reati informatici cambiano nel tempo – spiega Domenico Vulpiani, direttore del servizio di Polizia postale e delle Comunicazioni - negli ultimi anni sono diminuiti i casi di hakeraggio, contrastati dalla maggior parte degli antivirus che consentono una difesa concreta dell'utente. Sono aumentati, invece, i furti di identità e le clonazioni di carte di credito. L'attività di indagine in questi casi è complessa: i criminali concentrano le proprie attenzioni su molte vittime, prelevando ad ognuna poche migliaia di euro, utilizzando molti intermediari. A volte, alla fine delle indagini, è difficile recuperare i soldi delle vittime che, in genere, vengono fatti sparire con operazioni rapidissime. Nei casi di phishing il consiglio è sempre quello di non fornire via mail codici personali e password di accesso ai propri conti correnti: le banche ormai non rimborsano più le vittime di questi reati. E' sempre importante, poi, denunciare gli episodi alla polizia postale".

11 giugno 2009