INDICE

PROLOGO **3**

INTRODUZIONE **5**

CAPITOLO 1: TRUFFA AI DANNI DI PERSONE FISICHE **6**

CAPITOLO 2: TRUFFE IN PRIMA PERSONA **7**

2.01 - RICONTROLLARE I SOLDI 7
2.02 - RIPULIRVI LA GIACCA 7
2.03 - FALSE PIETRE PREZIOSE 7
2.04 - FALSA BENEFICENZA 8
2.05 - FALSA EREDITÀ 8
2.06 - FALSI FUNZIONARI INPS, ENEL O INPDAP 9
2.07 - SCHEMA DI PONZI 9

CAPITOLO 3: TRUFFE VIA INTERNET **11**

3.01 - FALSE OPERE DI CARITÀ 12
3.02 - LA TRUFFA DEL PREFISSO TELEFONICO 12
3.03 - LA TRUFFA NIGERIANA 13
3.04 - SPAM. 15
3.05 - SPAMMING ATTRAVERSO E-MAIL 17
3.06 - SPAMMING PER INTERPOSTA PERSONA 17
3.07 - TRUFFA DI VALENTIN 19
3.08 - SCAM 19
3.09 - SCAM SENTIMENTALI 20
3.10 -PHISHING 21
3.11 - SICUREZZA CARTE DI CREDITO 25
3.12 - BOXING 27
3.13- VISHING CARTE DI CREDITO 27
3.14 - WEBCAMMING O TRUFFA ATTRAVERSO LA WEBCAM 28

CAPITOLO 4: LE TRUFFE NEL MONDO DEL CINEMA **30**

4.01 - CONFIDENCE 30
4.02 - PROVA A PRENDERMI 33
4.03 - LA STANGATA 35
4.04 -IL GENIO DELLA TRUFFA 37

CAPITOLO 5: SECOND LIFE **39**

5.01 - CHE COS'È SECOND LIFE 39
5.02 - LE TRUFFE IN SECOND LIFE 41

CAPITOLO 6: CONCLUSIONI **51**

6.01 - COS'È L'XML? 51
6.02 - DESCRIZIONE DI UNA TRUFFA REALMENTE ACCADUTA 52
6.03 - ANALISI DELLA TRUFFA ATTRAVERSO L'EDITOR VXE 2.2 53
6.04 - ALBERO DEGLI ELEMENTI 55

RINGRAZIAMENTI **56**
NOTE **57**
BIBLIOGRAFIA **60**
FILMOGRAFIA **60**
SITI WEB **60**
PROGRAMMI **61**
INDICE FIGURE **61**

PROLOGO

La psicologia umana è assai complessa, ma ciò che caratterizza ogni uomo è l'incapacità di difendersi dal fascino del dio denaro. Spesso molte persone credono che la felicità si possa ottenere attraverso il denaro, per questo qualsiasi possibilità di guadagnare "soldi facili" si trasforma in una ghiotta occasione, l'uomo perde così di lucidità e diventa facilmente vulnerabile. Purtroppo vi sono molti individui meschini che approfittano di questa debolezza umana per arricchirsi a loro volta ideando le più svariate truffe. Anche in Italia il fenomeno delle truffe è assai sviluppato tanto che il quadro che emerge da uno studio condotto dal Centro Studi Temi della Confesercenti[1]. Un'Italia truffaldina che strumentalizza lo Stato e colpisce le imprese ed i cittadini onesti, ricorrendo a ingegnosi artifici e astuti stratagemmi che producono numerose illegalità. A cadere nel mirino dei truffatori sono soprattutto anziani, commercianti e piccole imprese. I numeri parlano chiaro: di circa 18 miliardi è il giro d'affari annuo che finisce nelle tasche di soggetti, raramente perseguiti dalla giustizia, che svolgono indisturbati il loro "sporco lavoro". Un settore in piena salute quello delle truffe, caratterizzato da una costante e inarrestabile crescita.

Una delle ultime frontiere delle frodi è quella del web: si chiamano phishing, boxing, skinning, trashing, termini inglesi che raccontano le azioni truffaldine che corrono sulla rete. Le truffe via internet sono in costante crescita: si calcola che dal 2005, ogni giorno, sono circa 8 milioni i tentativi di carpire dati e informazioni personali, attraverso una semplice mail, per accedere ai conti bancari di vittime ignare.

"I numeri e i denari movimentati - dichiara il presidente della Confesercenti, Marco Venturi - dimostrano che le truffe non sono più un reato "folkloristico" marginale, bensì una grave minaccia per le persone e per l'economia"[2].

Questo mio lavoro vuole essere una ricerca sui meccanismi e sull'analisi del percorso di truffa con il fine riuscire a trovare un metodo di studio per poter

schematizzare e catalogare le truffe, non solo nel mondo reale ma anche nel mondo virtuale di Second Life.

Inizialmente ho preso in esame la definizione di truffa e la nascita del termine a livello storico, successivamente ho concentrato la mia attenzione sul reato di truffa nel diritto italiano. Dopo aver introdotto abbastanza nel dettaglio le caratteristiche generali di tale reato ho esaminato le tipologie di truffe più diffuse. Ho cercato di analizzarle per poter delineare, anche attraverso l'utilizzo di mappe concettuali, le varie specifiche che determinano l'attenersi di una truffa in un determinato "gruppo di appartenenza". Su suggerimento del professor Giovanni Degli Antoni ho preso in esame anche alcuni film che trattassero il tema della truffa, in particolare ho analizzato i seguenti film: Confidence – film del 2003 - , Prova a prendermi – film del 2002 che si basa sulla vera storia di Frank William Abagnale [3] - , La stangata – film del 1973 – Il genio della truffa – film del 2003.

Dopo questo studio sulle truffe in senso lato ho focalizzato il mio lavoro su Second Life. In primo luogo ho voluto introdurre Second Life, cercando di spiegare i concetti e i meccanismi base di questo nuovo mondo virtuale. In fine ho fatto una piccola ricerca per verificare se anche questo mondo parallelo era soggetto a meccanismi di truffa..

Introduzione

"Dai tempi di "Totò Truffa" e "La banda dei Falsari" i tempi sono un po' cambiati. Con il passare degli anni i mezzi di comunicazione hanno contribuito all'evoluzione dei metodi adottati dai turlupinatori professionisti, da coloro, cioè, che fanno dell'ignoranza di poveri ingenui la propria ricchezza. Le truffe ispirano i registi a girare nuovi film da proiettare nelle sale cinema come i Confidence, Prova a Prendermi, La Stangata, Il Genio Della Truffa, per citarne alcuni, ma non ci tengono abbastanza aggiornati. Anche la televisione e i giornali arrivano troppo tardi perché descrivono l'evento solo dopo che lo stesso si è già verificato e le povere vittime possono solo sperare che si riesca a risalire al truffatore. Il mondo delle truffe è un mondo molto complesso e in continua evoluzione e come afferma Frank Abagnale :

> "*Ciò che feci io in gioventù è centinaia di volte più semplice oggi. La tecnologia alimenta il crimine."*

La nozione del delitto di truffa , il cui termine deriva dal tedesco "trug" (inganno, frode) è di formazione recente, poiché solamente nel secolo XIX tale illecito assunse una sua configurazione giuridica definita e autonoma. La prima nozione, sostanzialmente conforme a quella del diritto attuale, si ha nel 1819 nel codice penale francese il quale, nell'articolo 405 contempla il caso di colui che avrà "escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui"[4].

La truffa, nel diritto italiano, è un reato previsto dall'art.640 del codice penale ed è un esempio di reato a forma vincolata. È definita come attività ingannatoria capace di indurre la parte offesa in errore attraverso artifici e raggiri per indurla a effettuare atti di disposizione patrimoniale che la danneggiano e che favoriscono il truffatore o altri soggetti, procurando loro un profitto corrispondente al danno inferto alla vittima.

È un reato a dolo generico e di evento, cioè si consuma nel momento della verificazione dell'evento dannoso per la vittima e proficuo per il reo.

Capitolo 1: Truffa ai danni di persone fisiche

La truffa ai danni dei singoli, come quelle che colpiscono le società consistono in primo luogo nell'individuare le vulnerabilità della vittima (stato di salute fisico, psicologico, economico, preferenze personali) operando nelle seguenti tre fasi:

- Prima fase:
  raccolta illegale di informazioni personali (dati anagrafici, medici, abitudini quotidiane, età), con telefonate, pedinamento o interrogazione di vicini di casa impersonando pubblici ufficiali, amici, tecnici riparatori.
- Seconda fase:
  utilizzazione delle informazioni per scegliere la truffa che meglio si adatta alla vittima.
- Terza fase:
  scelta del momento e del luogo ideale, spesso un orario in cui un condominio o un vicinato sono meno frequentati o in cui la vittima è sola in casa, o se in piena strada, simulando una situazione di emergenza.

Le truffe più diffuse sono più spesso a danno di persone sole, anziani, ma anche coloro che soffrono di una situazione di disagio, malattia, o che non sono in grado di intendere e di volere e di conseguenza meno attente ai pericoli esterni.

Capitolo 2: Truffe in prima persona

2.01 Ricontrollare I Soldi

Alcuni tipi di truffa hanno come condizione iniziale che la vittima sia appena stata in banca o alla posta a ritirare dei soldi. Succede spesso che una persona anziana dopo aver fatto un prelievo venga seguita da qualcuno che poco dopo gli si presenta come funzionario di banca. In genere il finto funzionario suona al campanello di casa dicendo che potrebbe esserci stato un errore e che è necessario verificare il numero di serie delle banconote appena ritirate. Il truffatore, facendo finta di contarli o di controllarli, li sostituisce con banconote false.

2.02 Ripulirvi La Giacca

Ancora più diffusa e più vecchia è la truffa del gelato o del caffè sulla giacca. Sono nella maggior parte dei casi donne con bambini, ma a volte anche ragazzi, con il gelato o con un caffè in mano che urtano la vittima facendolo cadere sulla giacca. Poi con la scusa di ripulirla si impossessano del portafogli.

2.03 False Pietre Preziose

Una delle truffe più ricorrenti è la truffa delle false pietre preziose. Un signore di aspetto rassicurante e in genera di mezz'età, si finge uno straniero che per un'urgenza deve raggiungere il paese d'origine ma non ha disponibilità di soldi liquidi per il viaggio. Ferma una signora per strada e cerca di vendere un anello o delle pietre preziose che avrebbero un valore di 7/10mila euro. A questo punto interviene il complice, un altro signore ben

vestito che dice di essere un gioielliere con tanto di lente per controllare le pietre e subito dopo si offre di comprarle per 5mila euro. Ma lo straniero insiste perché sia l'anziana signora a comprarle e spesso riesce a convincerla facendosi dare 2/3mila euro.

2.04 Falsa Beneficenza

Un signore ben vestito, 50/60 anni circa, a volte con accento straniero, si finge un medico o un rappresentante di una casa farmaceutica alla ricerca di un deposito per effettuare una donazione di medicinali a scopo di beneficenza. Ferma un signore per strada, normalmente in quartieri borghesi, chiedendo informazioni su questo deposito: il signore ovviamente non sa niente. Arriva il complice che fa finta di sapere dove sia il deposito ma dice che è stato chiuso. La donazione allora può avvenire solo tramite notaio ma serve un anticipo in denaro che la persona incaricata della beneficenza non ha a disposizione in quel momento. L'anziano fermato per strada viene convinto che può contribuire alla beneficenza ricavando anche una percentuale se fornisce il denaro che serve per il notaio. Viene accompagnato a ritirare una discreta cifra e poi fatto salire sull'auto insieme ai due "compari" per andare dal notaio. Durante il tragitto i truffatori si ricordano che sicuramente servirà una marca da bollo. Si fermano davanti a un tabaccaio e chiedono alla vittima di andare a comprarla. Appena il truffato scende, naturalmente, fuggono.

2.05 Falsa Eredità

Stessa procedura per quanto riguarda una falsa eredità da consegnare. Un signore cerca un vecchio amico a cui dovrebbe consegnare del denaro relativo a un'eredità. Ferma una persona anziana per chiedere informazioni sull'amico, ma nessuno sa niente finché un passante, complice del tuffatore,

si ferma e dice che quella persona è morta. L'unica soluzione è il notaio ma serve l'anticipo.

2.06 Falsi funzionari Inps, Enel o Inpdap

Si presentano alla porta di persone anziane con la scusa di dover controllare la posizione pensionistica o contributiva; o ancora per controllare il contatore del gas, della luce ecc. ma in realtà raggirano le persone facendosi consegnare soldi o sottraendo beni o altre cose di valore.

2.07 Schema di Ponzi

Lo Schema di Ponzi è un modello economico di vendita truffaldino che promette forti guadagni alle vittime a patto che queste reclutino nuovi "investitori", a loro volta vittime della truffa.

Caratteristiche:

Lo Schema di Ponzi permette a chi comincia la catena e ai primi coinvolti di ottenere alti ritorni economici a breve termine, ma richiede continuamente nuove vittime disposte a pagare le quote. I guadagni derivano infatti esclusivamente dalle quote pagate dai nuovi investitori e non da attività produttive o finanziarie. Il sistema è naturalmente destinato a terminare con perdite per la maggior parte dei partecipanti, perché i soldi "investiti" non danno alcuna vera rendita né interesse, essendo semplicemente incamerati dai primi coinvolti nello schema che li useranno inizialmente per rispettare le promesse.

Le caratteristiche tipiche sono:

- Promessa di alti guadagni a breve termine
- Ottenimento dei guadagni da escamotage finanziari o da investimenti di "alta finanza" documentati in modo poco chiaro
- Rivolto ad un pubblico non competente in materia finanziaria
- Legato ad un solo promotore o azienda

Risulta evidente che il rischio di investimento in operazioni che sfruttano questa pratica è molto elevato. Il rischio è crescente al crescere del numero degli iscritti, essendo sempre più difficile trovare nuovi adepti. In Italia, USA e in molti altri stati, questa pratica è un reato, essendo a tutti gli effetti una truffa.

Storia:

La tecnica prende il nome da Charles Ponzi, un immigrato italiano in USA che divenne noto per avere applicato una simile truffa su larga scala nei confronti della comunità di immigrati prima e in tutta la nazione poi. Ponzi non fu il primo ad usare questa tecnica, ma ebbe tanto successo da legarvi il suo nome coinvolgendo 40000 persone e raccogliendo oltre 15 milioni di dollari.
Lo schema di Ponzi ha sviluppato nel tempo varianti più complesse, pur mantenendo la stessa base teorica e continuando a sfruttare l'avidità delle persone. Oggi esistono normative serie a riguardo per cui strutture con questi schemi risultano illegali in ogni parte del mondo tutelando sia l'incolumità delle persone sia quelle aziende che scelgano di avvalersi del marketing multilivello.

Esempio:
Un promotore promette guadagni fuori dagli standard su un investimento a breve termine, spesso riferendosi in termini fumosi a meccanismi complessi o inesistenti. Senza un investimento

documentato, solo pochi investitori danno fiducia al promotore, il quale si assicura di rispettare i patti: pagherà quanto pattuito, anche se lo farà andando in perdita o più spesso prelevando fondi versati da nuovi investitori. In seguito così potrà beneficiare della sua buona fama per far aumentare il capitale investito e il numero degli investitori, attirati dall'avidità.
I primi investitori, ripagati, reinvestiranno i fondi e parleranno bene dell'investimento attirando nuove vittime, fino a che il promotore, giunto al massimo del guadagno, sparirà nel nulla con i soldi presenti in quel momento. Spesso tuttavia la difficoltà di reperire nuovi adepti porterà lo schema a collassare da solo, non riuscendo a ripagare gli investimenti o venendo scoperto dalle forze dell'ordine.

3 Truffe via internet

Quando pensano ai crimini perpetrati in via internet,molti immaginano degli hacker che sottraggono numeri di carte di credito e poi spendono allegramente enormi somme di denaro che verranno poi rimborsate da qualcun altro. Anche se tutto ciò può avvenire, la minaccia più grave in internet non è rappresentata dagli hacker ma dai truffatori,molti dei quali non sono più competenti nell'utilizzo dei computer delle loro vittime.
Tutti i truffatori,indipendentemente dal fatto che stiano operando di persona, tramite posta, tramite il telefono o via internet, adottano lo stesso approccio di base.

- Promettono una fantastica ricompensa senza fatica o con poca fatica: le vittime spesso sono troppo accecate dall'ingordigia per domandarsi perché mai il truffatore dovrebbe offrire l'affare proprio a loro.
- Abusano della fiducia della vittima: i truffatori incoraggiano le vittime a dimostrare di meritare la ricompensa promessa.

- Raccolgono il denaro della vittime: i truffatori devono ingannare la vittime,la quale sarà convinta a cedere del denaro o qualcosa di prezioso.

Poiché tutti vorremmo poter guadagnare grandi somme di denaro senza lavorare,tutti siamo potenziali vittime delle truffe.

3.01 False Opere Di Carità

Queste truffe spesso coinvolgono siti web fasulli dall'aspetto apparentemente legittimo, che accettano pagamenti online, per esempio transazioni eseguite tramite Pay Pal. I siti web per false opere di carità possono attrarre coloro che vogliono donare denaro, ma i truffatori spesso si spingono un po' oltre e sollecitano attivamente le donazioni tramite lo spamming. Tali messaggi di posta elettronica non richiesti spesso menzionano il nome di un ente di carità dal nome molto simile a quello di un ente legittimo, come il National Heart Cancer Socety (al posto del legittimo America Heart Istitute).
Questi truffatori possono ingannarvi in due modi. Se donate i vostri soldi, invierete i vostri soldi a un truffatore invece che a sostegno delle vittime. Se invece fornite al truffatore il vostro numero di carta di credito, correte il rischio di subire grossi prelievi.

3.02 La Truffa Del Prefisso Telefonico

Alcune truffe contano sulla proliferazione di nuovi prefissi telefonici. Il truffatore lascia un messaggio telefonico o invia un messaggio di posta elettronica sostenendo che avete vinto un favoloso premio o che la vostra carta di credito ha subito un addebito errato o che un vostro parente è nei

guai, qualsiasi cosa che vi possa spingere a chiamare il numero di telefono o a rispondere al messaggio di posta elettronica.
Se chiamate il numero telefonico indicato nel messaggio, verrete messi in attesa. La persona che sta dall'altro capo del telefono ha il solo scopo di mantenervi in linea il più a lungo possibile poiché il numero telefonico è in realtà un servizio a pagamento che addebita al chiamante cifre astronomiche.

3.03 La Truffa Nigeriana

La truffa alla nigeriana è un raggiro informatico (ma che circola anche per posta ordinaria) tra i più diffusi al mondo inventato per la prima volta nel 1992 per lettera e nel 1994 per e-mail. Esistono centinaia di varianti a questa truffa, ma più o meno il senso è sempre lo stesso: uno sconosciuto non riuscirebbe a sbloccare un conto in banca di milioni di dollari, ed essendo lui un personaggio noto avrebbe bisogno di un prestanome discreto che compia l'operazione al suo posto.
Invita così alcuni utenti concedendo loro questa possibilità in cambio di una promessa fetta del bottino. La truffa è chiamata anche 419 scam (419 è il riferimento numerico della legge nigeriana, disinvoltamente ignorata dai nigeriani, che rende illegali questi inviti).
È facile capire che questo è solo un tentativo di truffa:

- Il rischio di coinvolgere uno sconosciuto in un affare simile è alto, perché potrebbe compromettere la riservatezza dell'operazione.
- L'invio in rete non è intrinsecamente sicuro, per cui l'inoltro via e-mail non è un veicolo credibile per un affare di questo tipo.
- Gli "inviti" che circolano sono moltissimi, e tutti uguali.
- La letteratura online su questi casi è ricca e documentata.
- L'occasione è troppo bella per essere vera, e il mittente mette pressione alla vittima per concluderla.

Gli effetti per chi cade nella trappola seguono un copione prestabilito: prima vengono chiesti soldi per la parcella del notaio, poi altro denaro per l'avvocato ed infine si viene invitati ad un incontro personale nella loro nazione (di solito la Nigeria, da cui il nome di "truffa alla nigeriana", ma spesso anche in paesi terzi come l'Italia. Milano è un luogo scelto di frequente per la sua vicinanza all'Europa). Arrivati nel luogo dell'appuntamento, possono accadere due cose: o si viene accolti in modo opulento dando al truffato l'impressione della veridicità dell'affare, o si viene direttamente rapinati se le prospettive non sono buone per eventuali guadagni maggiori. In entrambi i casi, i ladri hanno raggiunto il loro scopo.
Questo imbroglio può anche finire in tragedia: nel 2003 Michael Lekara Wayid, diplomatico nigeriano in Repubblica Ceca, è stato ucciso a colpi di fucile da un ultrasettantenne furioso per essere stato raggirato con questo sistema. Nel 2002 un inchiesta giornalistica stimò in almeno 15 gli omicidi relativi alle "truffe nigeriane".

Meccanismi della truffa:

Gli 'investitori solitamente vengono contattati con un'offerta di questo tipo: "In questo paese povero ci sarebbe una persona molto ricca che avrebbe bisogno di spostare all'estero del denaro con la massima discrezione, sarebbe possibile utilizzare il suo conto?".
Le somme coinvolte sono normalmente nell'ordine dei milioni di dollari, e all'investitore viene promessa una forte percentuale, spesso del 40%. L'accordo proposto è spesso presentato come un crimine innocuo, in modo da dissuadere i partecipanti dal contattare le autorità. In Nigeria l'operazione è organizzata professionalmente, con uffici, numeri di fax funzionanti e spesso con contatti in uffici governativi. Gli investitori che cercano di scoprire cosa si trova a monte dell'offerta, spesso trovano un sistema organizzato, in cui tutti i pezzi si combinano perfettamente.
Nel momento in cui la vittima accetta di partecipare all'affare, il truffatore per prima cosa invia alcuni documenti fasulli che portano impressi timbri e

sigilli ufficiali del governo, o in alternativa manda alcune mail per informare il socio dei "progressi". Presto però inizia a parlare di ritardi, relativi a necessità di corruzione o pratiche burocratiche che richiedono un grosso anticipo in denaro. Le scadenze vengono via via prorogate e i costi aumentano, ma viene mantenuta viva la promessa dell'imminente trasferimento di denaro. La pressione psicologica è mantenuta alta, per stimolare il truffato a concludere in fretta senza coinvolgere altre persone. In alcuni casi le vittime sono invitate in Nigeria per incontrare funzionari governativi, spesso falsi. Alcune vittime una volta giunte vengono addirittura prese in ostaggio fino al pagamento di un riscatto, o sono portate nel paese in modo illecito senza visto di ingresso e poi ricattate per poterne uscire. Nei casi più estremi la vittima può essere anche uccisa.

3.04 Spam

Il termine trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam (un tipo di carne in scatola). Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con "spam" ("uova e spam, uova pancetta e spam, salsicce e spam" e così via) si contrappone alla riluttanza del cliente per questo alimento. I Monty Python prendono in giro la carne in scatola Spam per l'assidua pubblicità che la marca era solita condurre, da qui lo sketch dei Monty's e successivamente l'adattamento informatico alla pubblicità non desiderata.
Si ritiene che il primo spam via email della storia sia stato inviato il 1 maggio 1978 dalla DEC per pubblicizzare un nuovo prodotto. Nella terminologia informatica le spam possono essere designate anche con il sintagma di junk-mail, che letteralmente significa posta-spazzatura.

Scopi:

Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Uno spammer, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi sono spesso raccolti in maniera automatica dalla rete o ottenuti da database o semplicemente indovinati usando liste di nomi comuni.

Per definizione lo spam viene inviato senza il permesso del destinatario ed è un comportamento ampiamente considerato inaccettabile dagli Internet Service Provider (ISP) e dalla maggior parte degli utenti di Internet. Mentre questi ultimi trovano lo spam fastidioso e con contenuti spesso offensivi, gli ISP vi si oppongono anche per i costi del traffico generato dall'invio indiscriminato. Un gran numero di spammer utilizza intenzionalmente la frode per inviare i messaggi, come l' uso di informazioni personali false (come nomi, indirizzi, numeri di telefono) per stabilire account disponibili presso vari ISP. Per fare questo vengono usate informazioni anagrafiche false o rubate, in modo da ridurre ulteriormente i loro costi.

Questo permette di muoversi velocemente da un account a un altro appena questo viene scoperto e disattivato dall'ISP. Gli spammer usano software creato per osservare connessioni Internet con scarsa sicurezza, che possono essere facilmente dirottate in modo da immettere i messaggi di spam direttamente nella connessione dell'obiettivo con il proprio ISP. Questo rende più difficile identificare la posizione dello spammer e l'ISP della vittima è spesso soggetto di aspre reazioni e rappresaglie da parte di attivisti che tentano di fermare lo spammer.

I mittenti di e-mail pubblicitarie affermano che ciò che fanno non è spamming. Quale tipo di attività costituisca spamming è materia di dibattiti, e le definizioni divergono in base allo scopo per il quale è definito, oltre che

dalle diverse legislazioni. Lo spamming è considerato un reato in vari paesi e in Italia l'invio di messaggi non sollecitati è soggetto a sanzioni.

3.05 Spamming attraverso E-Mail

I più grandi ISP come America On-Line riferiscono che una quantità che varia da un terzo a due terzi della capacità dei loro server di posta elettronica viene consumata dallo spam. Siccome questo costo è subito senza il consenso del proprietario del sito, e senza quello dell'utente, molti considerano lo spam come una forma di furto di servizi. Molti spammer mandano i loro messaggi attraverso gli open mail relay. I server SMTP, usati per inviare e-mail attraverso internet, inoltrano la posta da un server a un altro; i server utilizzati dagli ISP richiedono una qualche forma di autenticazione che garantisca che l'utente sia un cliente dell'ISP. I server open relay non controllano correttamente chi sta usando il server e inviano tutta la posta al server di destinazione, rendendo più difficile rintracciare lo spammer.

3.06 Spamming per interposta persona

Lo spamming per interposta persona è un mezzo più subdolo utilizzato sfruttando l'ingenuità di molta gente. Per l'esattezza si intende di solito l'invio di Email commerciali ad alcuni destinatari conosciuti e magari regolarmente iscritti ad una newsletter dello spammer invitandoli a far conoscere una certa promozione ad uno o più persone conosciute dall'ingenuo destinatario, invogliandolo magari con qualche piccolo compenso.
Grazie a questo sistema sarà l'ingenuo destinatario a “spammare” altre caselle di posta di suoi conoscenti e quindi coprendo colui che c'è dietro e che guadagnerà da questo comportamento.

I costi :

Lo spamming è a volte definito come l'equivalente elettronico della posta-spazzatura (junk mail). Comunque, la stampa e i costi postali di questa corrispondenza sono pagati dal mittente - nel caso dello spam, il server del destinatario paga i costi maggiori, in termini di banda, tempo di elaborazione e spazio per immagazzinamento. Gli spammer usano spesso abbonamenti gratis, in modo tale che i loro costi siano veramente minimi. Per questa ricaduta di costi sul destinatario, molti considerano questo un furto o un equivalente di crimine. Siccome questa pratica è proibita dagli ISP, gli spammer spesso cercano e usano sistemi vulnerabili come gli open mail relay e server proxy aperti. Essi abusano anche di risorse messe a disposizione per la libera espressione su internet, come remailer anonimi. Come risultato, molte di queste risorse sono state disattivate, negando la loro utilità agli utenti legittimi.

Economia:

Siccome lo spam è economico da inviare, un ristretto numero di spammer possono saturare Internet con la loro spazzatura. Nonostante solo un piccolo numero dei loro destinatari sia intenzionato a comprare i loro prodotti, ciò consente loro di mantenere questa pratica attiva. Inoltre, sebbene lo spam appaia per una azienda rispettabile una via economicamente non attuabile per fare business, è sufficiente per gli spammer professionisti convincere una piccola porzione di inserzionisti ingenui che è efficace per fare affari.

3.07 Truffa di Valentin

La truffa di Valentin è un raggiro informatico applicato per la prima volta nel novembre del 1999 da uno spammer russo residente a Kaluga che si presentava col nome Valentin Mikhaylin (poi cambiato in Valentin Mikhailyn, Walentin Mihailin e simili). Questa truffa rientra nel genere delle truffe alla nigeriana.

Tramite la tecnica dello spam vengono inviate migliaia di e-mail che presentano una storia straziante: Valentin afferma di essere molto povero, di avere una madre (di nome Elena) malata e di non riuscire a sopportare il terribile inverno russo, per cui chiede dei soldi da inviare ad un indirizzo privato, o l'invio di CD musicali per poterli scambiare con denaro.

Un lavoro di inchiesta svolto dal debunker Paolo Attivissimo[5] ha portato ad una migliore comprensione della truffa, già nota ed in corso da anni, anche grazie a degli indizi che lo spammer non è riuscito a nascondere.

Nel 2006 Valentin è tornato in azione, stavolta con il nome di "Walentin", con truffe basate sullo stesso meccanismo: il motivo del cambio del nome è da ricercare nella sua intenzione di non farsi trovare nelle ricerche compiute su Google dagli utenti insospettiti dai suoi messaggi.

3.08 Scam

Scam è un termine che indica un tentativo di truffa con i metodi dell'ingegneria sociale effettuato in genere inviando una e-mail nella quale si promettono grossi guadagni in cambio di somme di denaro da anticipare. Spesso scam e spam sono strettamente correlati.

Tipico e forse primo esempio, la truffa alla nigeriana. Nella e-mail si parla di grosse somme di denaro che dovrebbero essere trasferite o recuperate da una banca estera la quale però chiede garanzie, come la cittadinanza, un conto corrente, un deposito cauzionale. Chi scrive perciò chiede il vostro

aiuto sia per trasferire il denaro tramite il vostro conto che per anticipare il deposito cauzionale. Come ricompensa si riceverà una percentuale del denaro recuperato. Altri esempi di scam prospettano una vincita alla lotteria ma per ritirare l'immaginario premio si dovrà versare una tassa.

3.09 Scam sentimentali

Un'altra forma di Scam, questa volta ben più subdola, avviene tramite siti internet per incontri e conoscenze. Alcune donne, di varia provenienza come est Europa, Russia e persino Africa, mandano un messaggio di interesse alla vittima. Si istaura così un rapporto a distanza tramite email con un fitto scambio di corrispondenza. La donna, in genere si presenta con un profilo e un'immagine avvenente e con un atteggiamento subito propenso alla costruzione di un rapporto sentimentale. Sempre disponibile al dialogo, invia in genere foto a bassa risoluzione, a volte palesemente scaricate da internet, per cui identificabili come fasulle. Dopo un certo lasso di tempo però viene richiesta una somma di denaro per far fronte a problemi economici, come un'improvvisa malattia, un prestito in scadenza ecc. La vittima, viene quindi convinta a trasferire una certa cifra tramite conto bancario o con un trasferimento di contanti tipo Western Union. Subito dopo aver incassato i soldi la donna fa perdere i propri contatti.
Per prevenire questo tipo di truffe è utile tenere conto di alcuni elementi comuni che devono far insospettire:

- rapido interesse della persona nei vostri confronti, anche con la possibilità di un matrimonio
- le foto inviate sono spesso a bassa risoluzione (come fossero già preparate) e a volte palesemente scaricate da internet
- le donne sono spesso avvenenti
- richiesta di soldi, per un quantitativo non troppo elevato

3.10 Phishing

In ambito informatico il phishing ("spillaggio di dati sensibili", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.
La prima menzione registrata del termine phishing è sul newsgroup di Usenet il 2 gennaio 1996, malgrado il termine possa essere apparso precedentemente nell'edizione stampata della rivista per hacker 2600. Il termine phishing è una variante di fishing (letteralmente "pescare" in lingua inglese), probabilmente influenzato da phreaking e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente.

Metodologia di attacco:

Il processo standard delle metodologie di attacco di spillaggio può riassumersi nelle seguenti fasi:

- l'utente malintenzionato (phisher) spedisce al malcapitato ed ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
- l'email contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account ecc.).
- l'email invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua

posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione.

- il link fornito, tuttavia, non porta in realtà al sito web ufficiale, ma ad una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere ed ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
- il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Talora, l'email contiene l'invito a cogliere una nuova "opportunità di lavoro", a dare le coordinate bancarie del proprio conto online per ricevere l'accredito di somme che vanno poi trasferite ad altri conti, trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. Solitamente, il trasferimento avviene con bonifici gratuiti, sempre via Internet, verso un altro conto online.
Si tratta del denaro rubato con lo spillaggio, per il quale il titolare del conto online, spesso in buona fede, commette il reato di riciclaggio di denaro sporco. Questa attività comporta per il phisher la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste comunque un interesse a disperdere il denaro in molti conti correnti e a fare girate in differenti Paesi, perché diviene più difficile risalire al suo conto e dati identificativi. Se i trasferimenti coinvolgono più Paesi, i tempi per la ricostruzione dei movimenti bancari si allungano, poiché serve una rogatoria e l'apertura di un procedimento presso la magistratura locale di ogni Paese interessato.

Esempio di phishing ai danni dei clienti di Banca Intesa:

Figura 1: Esempio phishing Banca Intesa

Esempio di phishing ai danni dei clienti di Poste Italiane:

Figura 2: Esempio phishing Poste Italiane

3.11 Sicurezza carta credito

E' possibile individuare diversi tipi di truffe che hanno come oggetto le carte di credito e della carta di debito:

Phising carta di credito:

Il Phising è una frode on-line ideata per sottrarre con l'inganno numeri di carte di credito e password. Generalmente si viene contattati tramite e-mail che sembrano provenire da siti web autentici o noti, come quello della propria banca, i quali richiedono all'utente l'inserimento di informazioni personali. Di recente è stato escogitato anche il phishing via sms sul cellulare.

Skimming:

Lo Skimming è il processo con il quale i dati contenuti nella banda magnetica di una carta di credito sono copiati in un'altra carta di credito falsa tramite un apparecchio chiamato skimmer i truffatori si impossessano dei dati, li riportano poi su computer e li trascrivono su altre carte di credito. Con la sostituzione della banda magnetica con un microchip, i malfattori non potranno più servirsi di tale metodo per impossessarsi dei dati.

Trashing:

Con il Trashing i truffatori cercano gli scontrini delle carte di credito gettati via dopo un acquisto, oppure gli estratti conto della carta di credito buttati dentro la spazzatura. Attraverso questi documenti cercano di ricostruire i dati dell'utente.

Sniffing:

Si tratta di una tecnica per intercettare le coordinate di pagamento durante un acquisto on line. Questa tecnica è molto complessa ed è attuata da professionisti hacker. Vengono utilizzati degli strumenti per intercettare il traffico dell'utente. Lo strumento principale è lo sniffer.
Uno sniffer è un qualsiasi strumento, sia esso un software o un apparato hardware, che raccoglie le informazioni che viaggiano lungo una rete (network). Questa rete può utilizzare un protocollo di comunicazione qualunque: Ethernet, TCP/IP (Internet si basa principalmente su questo protocollo), IPX o altri. Generalmente si utilizzano software sniffer e il termine in questione si riferisce a The Sniffer Network Analyzer, il nome del primo programma di questo tipo, sviluppato dalla Network Associates Inc. è protetto da trademark.
Tuttavia la parola "sniffer" è ora di uso comune come PC o kleenex e con essa ci riferiamo a tutti i programmi che implementano quelle stesse funzioni. Si possono dividere i vari tipi di sniffer in due grandi branche:

- i prodotti commerciali che sono rivolti agli amministratori di rete e alla manutenzione interna delle reti stesse;
- i prodotti sviluppati nell'underground informatico, spesso dotati di un'incredibile varietà di funzioni ulteriori rispetto ai tool commerciali.

Entrambi possono essere utilizzati come mezzo per accedere ad una rete. Se vogliamo fare una distinzione che non si basi solo sul prezzo del prodotto o sulla sua provenienza, possiamo considerare i software precedenti come un tutt'uno e rapportarli ad applicativi come gli analizzatori di rete (network analyzer) che danno la possibilità di fare qualche operazione in più rispetto al semplice ascolto e archiviazione dei dati di passaggio su una rete, come compilare statistiche sul traffico e sulla composizione dei pacchetti.

Le funzioni tipiche degli sniffer non differiscono di molto e possono essere riassunte sinteticamente in: filtraggio e conversione dei dati e dei pacchetti in una forma leggibile dall'utente, analisi dei difetti di rete.
Ad esempio:

- analisi di qualità e portata della rete (performance analisys)
- setacciamento automatizzato di password e nomi di utenti (in chiaro o, più spesso, cifrati) per successiva analisi
- creazione di log, lunghi elenchi che contengono la traccia, in questo caso, del traffico sulla rete
- scoperta di intrusioni in rete attraverso l'analisi dei log del traffico Si tratta di una tecnica per intercettare le coordinate di pagamento durante un acquisto on line.

3.12 Boxing:

Una tipologia di truffa in netta crescita negli anni è quella detta del boxing. Lo scopo è comunque quello di clonare carte di credito e bancomat, ed il prerequisito necessario è quello di reperire in maniera illecita dati personali appartenenti a legittimi titolari.
Il boxing consiste nella sottrazione delle carte di credito inviate dalle banche ai loro clienti, proprio intercettando le stesse nelle cassette della posta.

3.13 Vishing carte magnetiche:

Vishing è una truffa che si serve di un finto servizio di notifica d'acquisto via sms . L'sms, che ha un testo sempre diverso, notifica un problema durante un acquisto con carta di credito, ed invita a chiamare un numero che inizia per 8(es. 800-50500) il costo che viene addebitato è di circa 15 euro, spesso la telefonata invita ad inserire un codice o il proprio numero di carta di credito, la comunicazione viene poi fatta cadere e costringe il truffato ad effettuare una seconda telefonata, vedendosi addebitare altri 15 euro oppure

il numero inizia per 0 (es. 011-1234567 - come una normale telefonata urbana) alla quale risponde un operatore che conferma lui stesso il numero della carta di credito e chiede che gli vengano forniti gli altri dati per conferma, come il nome e cognome, la scadenza e i tre numeri posti sul retro della carta.

3.14 Webcamming o truffa attraverso la webcam

Attraverso dei particolari virus un hacker può impossessarsi della webcam dell'utente e trasmettere alla sua insaputa le immagini che riesce a carpire.
Questa truffa è subdola perché con pazienza l'hacker raccoglie materiale violando la vostra privacy in attesa di qualsiasi dato che lo possa aiutare a scoprire i vostri accessi ai conti o quant'altro possa essere utile ad acquisire denaro.

Violazioni della privacy:

Questa truffa è spiacevole anche dal punto di vista della privacy, avere un occhio elettronico puntato addosso che vi spia senza che lo sappiate è una grave violazione dei diritti dell'individuo. Alcuni hacker hanno come obiettivo non la truffa in termini economici ma il semplice ma ugualmente spiacevole istinto voyeuristico di vedere immagini di ragazze o donne. In alcuni casi vendono poi le immagini in webcam delle ragazze, soprattutto le più belle e attraenti.

Ecco le ultime truffe tramite Webcam:

Alcune persone vengono spiate dalla loro webcam e non lo sanno. Un utente spagnolo, per caso, si è accorto di avere sul proprio PC un file che non riconosceva. Ha segnalato la cosa alla Polizia che, dopo aver compiuto degli accertamenti, ha capito che si trattava di un virus

appositamente scritto, e diffuso su reti P2P, per poter controllare la webcam. L'autore del virus è stato individuato ed arrestato, si tratta di un 37enne spagnolo che è stato riconosciuto colpevole di aver rubato le password di sistemi di e-banking e di aver scritto un virus in grado di spiare le vittime attraverso le loro webcam. Il virus in questione veniva diffuso attraverso piattaforme Peer to Peer come file musicale o immagine. Gli esperti fanno notare che esistono circa 200 virus che hanno questo potere e che, sfruttando la scarsa preparazione degli utenti, si installano sul PC della vittima senza che questi se ne renda neanche conto.

Capitolo 4: Le truffe nel mondo del cinema

Dopo aver analizzato le diverse tipologie di truffa nel mondo reale, ho spostato la mia attenzione sulla rappresentazione, riproduzione cinematografica delle truffe per poter analizzare meglio il percorso di truffa, cercando di individuarne le fasi principali. Ho preso in esame quattro film, uno degli anni '70 e i restanti dei primi anni del 2000.

4.01 Confidence

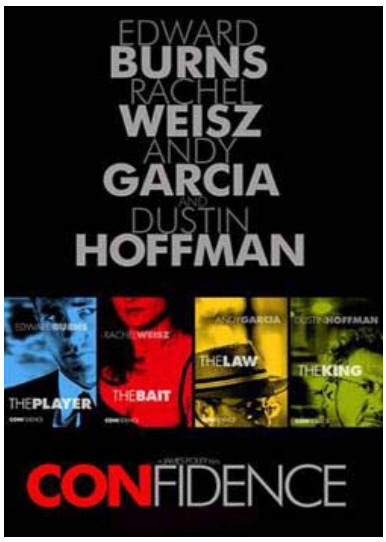

Figura 3: Locandina Confidence

Titolo originale:	Confidence
Nazione:	Usa/Canada/Germania
Anno:	2003
Genere:	Thriller
Regia:	James Foley
Cast:	Edward Burns, Rachel Weisz, Andy Garcia, Dustin Hoffman, Paul Giamatti
Produzione:	Michael Burns, Marc Butan, Michael Ohoven

Trama:

Jake Vig è un giovane truffatore, ingegnoso e ricco di charme. Per svolgere degnamente il proprio mestiere ha bisogno di compari altrettanto abili e soprattutto affidabili. Quando però si ritrova a dover fare i conti con il Re, un truffatore, sadico e avido, che controlla una vasta zona cittadina, iniziano i guai e per uscirne Jake e i suoi devono mettere a segno un colpo milionario a danno di un vecchio rivale del Re.

Analisi del processo di truffa:

Dall'analisi delle truffe messe in atto in questo film si può dedurre che i truffatori inizialmente hanno come unico fine il denaro, successivamente però subentra il bisogno di sfidare gli altri e di provare emozioni cariche di adrenalina. I truffatori, prima di agire, devono organizzare con estrema attenzione e precisione sia la composizione della loro "banda" che i diversi passaggi del loro piano. Per definire la cosiddetta banda devono scegliere gli elementi più adatti per ogni incarico e dividersi i propri ruoli. In questo film la truffa viene definita come una recita dove ognuno ha la propria parte; in particolare i ruoli sono:

- il truffatore
- il compare
- il ponte
- l'appoggio
- la vittima

Ognuno di loro, esclusa ovviamente la vittima, ha dei compiti precisi, delle mosse e delle battute già studiate e stabilite in ogni minimo dettaglio. Una volta delineata la "banda" viene scelta la vittima la quale deve possedere determinate caratteristiche: deve essere un individuo, preferibilmente uomo poiché risulta meno complicato confonderlo e convincerlo con l'ausilio di

una "donna ammaliatrice", il quale non ha niente da perdere in quanto conduce una vita monotona e con poca vita sociale; le persone sole sono le vittime migliori. Un'altra caratteristica che deve avere la vittima prescelta è la bramosia di denaro, la convinzione che i soldi diano potere e felicità e che grazie ad essi si può tutto, caratteristica che inconsapevolmente è intrinseca nell'uomo.
In questo film il percorso di truffa si delinea attraverso delle tappe predefinite:

- instaurare un rapporto di fiducia tra truffatore e vittima: il truffatore è il classico "ragazzo dalla faccia pulita" educato e gentile.
- far credere alla vittima che sta compiendo una buona azione: il truffatore, che ora agli occhi della vittima risulta essere una persona per bene, confida al mal capitato di essere in difficoltà e di aver bisogno di un piccolo favore.
- promettere al mal capitato che riceverà una ricompensa per l'aiuto offerto.

Il truffatore riesce ad ingannare la vittima ed a mettere in atto la truffa grazie alla sua abilità nel mentire, barare e manipolare.

Mentire = affermare il falso consapevolmente
Barare = comportarsi in modo disonesto
Manipolare = condizionare, manovrare

Nello svolgimento di una truffa ci possono essere degli imprevisti, un buon truffatore deve saper prevedere ogni possibile mossa, come in una partita di scacchi. I truffatori devono essere assistiti anche da una buona dose di fortuna e devono essere in grado di mantenere calma e sangue freddo in ogni circostanza.

4.02 Prova a prendermi

Figura 4: Locandina Prova a prendermi

Titolo originale:	Catch me if you can
Nazione:	Usa
Anno:	2002
Genere:	Azione
Regia:	Steven Spielberg
Cast:	Leonardo DiCaprio, Tom Hanks, Christopher Walken, Jennifer Garner, Amy Adams, Ellen Pompeo
Produzione:	Walter F. Parkes, Steven Spielberg

Trama:

Figura 5: Frank W. Abagnale

Frank W. Abagnale[3] è un uomo dalle mille identità: prima di compiere ventun'anni è già stato medico, avvocato e pilota di linea. Maestro nell'arte

della truffa Frank è un falsario coi fiocchi ed è riuscito ad intascare una fortuna grazie alla sua straordinaria abilità nella frode finanziaria. Per l'agente dell'FBI Carl Hanratty catturare Frank e assicurarlo alla giustizia è diventato un chiodo fisso, ma l'abile imbroglione lo batte sempre sul tempo, costringendolo a continuare l'inseguimento.

Analisi del processo di truffa:

Dall'analisi delle truffe messe in atto in questo film si può dedurre che il truffatore ha come fine il denaro, per arricchirsi personalmente e per salvare i suoi genitori. Il truffatore agisce sempre da solo, senza l'aiuto di nessun complice; egli ha un grande spirito di osservazione e una spiccata intelligenza, incanta le sue vittime con gentilezza ed educazione.
Non segue un piano ben definito, ma approfitta di ogni occasione per mettere in atto una nuova truffa utilizzando l'improvvisazione. Alla base di tutte i suoi inganni c'è la falsificazione di assegni, attestati e documenti.

4.03 La stangata

Figura 6: Locandina La stangata

Titolo originale: The sting

Nazione:	Usa
Anno:	1973
Genere:	Drammatico / Avventura
Regia:	George Roy Hill
Cast:	Paul Newman, Robert Redford, Robert Shaw, Charles Durning, Ray Walston, Eileen Brennan, Harold Gould, John Heffernan
Produzione:	Bill Philips

Trama:

Negli anni trenta i gangster dominano la scena, ma Henry e Jonny invece della pistola preferiscono usare l'astuzia. Organizzano così una colossale truffa ai danni del boss locale che ci rimetterà un sacco di dollari..

Analisi del processo di truffa:

Dall'analisi delle truffe messe in atto in questo film si può dedurre che il truffatore ha come fine principale il denaro, si ritiene un'artista e mai potrebbe trovare un occupazione diversa poiché nessun lavoro è altrettanto eccitante e rischioso. Bisogna però aggiungere decide di mettere in atto una "supertruffa" per vendicarsi della morte di un amico.
Come prima mossa il truffatore seleziona i diversi componenti delle "banda"e inizia a studiare le caratteristiche dell'uomo che deve truffare, è alla ricerca del suo punto debole.
La truffa è una vera e propria recita in cui viene realizzata anche l'ambientazione, i truffatori per ingannare la vittima organizzano delle "prove"in cui però il mal capitato ottiene dei benefici economici. Ogni gesto ed ogni azione è studiata nel minimo dettaglio, tutto deve essere perfetto.

4.04 Il genio della truffa

Figura 7: Locandina Il genio della truffa

Titolo originale: Matchstick Men

Nazione:	Usa
Anno:	2003
Genere:	Commedia
Regia:	Ridley Scott
Cast:	Nicolas Cage, Sam Rockwell, Alison Lohman, Bruce McGill
Produzione:	Sean Bailey, Ted Griffin, Jack Rapke, Ridley Scott, Steve Starkey, Robert Zemeckis

Trama:

Roy e Frank sono una coppia di truffatori da strapazzo, ma la loro "società" è fruttuosa. Nella vita privata Roy non ha altrettanto successo. Ci sta poco con la testa ed è costretto a ricorrere a uno psicanalista. Scopre che ha una figlia adolescente, Angela, e la routine meticolosamente ordinata si infrange. Mentre egli matura sentimenti paterni per la quattordicenne, lei è attratta dalla discutibile carriera del paparino. Angela vuole far parte della

società. Ma la cosa potrebbe mettere seriamente in pericolo la salute mentale di Roy, e il suo stile di vita...

Analisi del processo di truffa:

Dall'analisi delle truffe messe in atto in questo film si può dedurre che, anche in questo caso, i truffatori hanno come fine ultimo il denaro. Il meccanismo di truffa consiste nello studiare la vittima e nell'organizzare un piano talmente flessibile da poter essere modificato per qualsiasi evenienza. Il truffatore si considera un vero artista che però deve tenersi in allenamento per non commettere nessun tipo di errore o imprecisione; per fare ciò si esercita facendo delle prove di recitazione davanti allo specchio per trovare l'atteggiamento e l'abbigliamento migliore per risultare convincente e credibile. Il truffatore non deve mai perdere di vista l'obiettivo e deve fare in modo che nessuno si interponi tra lui e la vittima.

Dopo aver analizzato i vari aspetti delle truffe nella vita reale, su suggerimento del Professor Degli Antoni, ho spostato la mia attenzione sul mondo virtuale ed in particolare su Second Life.
Prima di affrontare il tema della truffa ritengo opportuno introdurre brevemente alcune nozioni su Second Life.

5 Second Life

5.01 Che cos'è Second Life?

Figura 8: Logo Second Life

Second Life è un mondo virtuale tridimensionale multi-utente online inventato nel 2003 dalla società americana Linden Lab[6].

A prima vista, Second Life richiama alla mente i videogames online, ma, al contrario dei videogames, non c'è nessuna struttura narrativa predefinita, non ci sono percorsi obbligati, non c'è un nemico da combattere, non ci sono regole del gioco. In Second Life, il gioco è solo una delle attività possibili. Il sistema fornisce ai suoi utenti (definiti "residenti") gli strumenti per aggiungere e creare nel "mondo virtuale" di Second Life nuovi contenuti grafici: oggetti, fondali, fisionomie dei personaggi, contenuti audiovisivi, ecc. La peculiarità del mondo di Second Life è quella di lasciare agli utenti la libertà di usufruire dei diritti d'autore sugli oggetti che essi creano, che possono essere venduti e scambiati tra i "residenti" utilizzando una moneta virtuale (il Linden Dollar[7]) che può essere convertito in veri dollari americani e anche in Euro.

"Non sto costruendo un nuovo gioco, ma un nuovo Paese".

Philip Rosedale aveva già le idee chiare, quando nel 1999 fondò a San Francisco la società Linden Lab. onario.

Attualmente partecipano alla creazione del mondo di Second Life oltre 450.000 utenti attivi di tutto il pianeta, e ciò che distingue "Second Life" dai normali giochi 3D online è che il contenuto di Second life è creato dagli utenti stessi. Gli incontri all'interno del mondo virtuale appaiono dunque come reali scambi tra esseri umani attraverso la mediazione “figurata” degli avatar.

Figura 9: Immagini Second Life

L'iscrizione è gratuita, ed è necessario essere maggiorenni per entrare nella grid principale. I minorenni che si registrano a SecondLife possono entrare soltanto nella Teen Grid, appositamente creata per i minorenni. Per possedere terreno in Mainland, cioè direttamente gestito da LindenLab, all'interno di “Second Life”, bisogna essere registrati come utenti “premium” mentre per creare o vendere oggetti basta l'iscrizione gratuita (Basic - Free). Molti personaggi che partecipano alla vita di “Second Life” sono programmatori in 3D. Qualcuno di essi ha guadagnato somme di (vero) denaro vendendo gli script dei propri oggetti creati per essere utilizzati dentro il mondo virtuale.

Second Life viene comunemente utilizzato dai suoi utenti per proporre agli altri partecipanti conferenze, file musicali e video, opere d’arte, messaggi

politici, ecc.; si è inoltre assistito alla creazione di numerose sottoculture all'interno dell'universo simulato, che è stato studiato in numerose università come modello virtuale di interazione umana.

5.02 Le truffe in Second Life

Riassumendo Second Life è una comunità virtuale in 3D, un nuovo mondo o una seconda opportunità, dove chiunque può realizzare il proprio alter ego così come avrebbe voluto essere nella vita reale e dare vita ad una nuova esistenza, con la possibilità di costruirsi un proprio avatar, ovvero un personaggio a cui si può dare le sembianze che più aggrada, e di essere catapultati all'interno di un vero e proprio mondo virtuale il cui unico scopo è "vivere". Una sorta di valvola di sfogo dove è possibile condurre la vita che si è sempre sognato: cantante, pittore, miliardario e perché no, anche un cyber criminale[8].

Come dichiarato sul sito ufficiale dai creatori di Second Life: "In Second Life, così come nel Mondo Reale, ci sono molte opportunità per l'innovazione ed il profitto . Aprire un nightclub, vendere gioielli, diventare un agente immobiliare."

L'importanza di Second Life e la sua indiscussa popolarità è stata presto capita da molte persone; solo due esempi su tutti: la Svezia ha aperto un'ambasciata virtuale e Microsoft ha pubblicizzato Visual Studio[9] su Second Life.

Parlando delle opportunità di lavoro è giusto precisare che, in generale, le grandi aziende cercano, in primis, di pubblicizzare i loro prodotti su Second Life, mentre le piccole imprese ed i privati provano a fare affari nel mondo virtuale in modo tale da guadagnare soldi reali.

Sfortunatamente, qualunque sia l'occasione per fare soldi, sia essa reale o virtuale, esiste un cyber criminale pronto a cercare metodi e strategie per trarre dei vantaggi dalla situazione.

E' per questo motivo interessante notare come la libertà concessa ai videogiocatori abbia dato anche la libertà di commettere reati all'interno del mondo virtuale di Second Life, a tal punto che sono nate associazioni come la criminalità virtuale organizzata infatti esistono "uffici" in cui ogni residente può richiedere i servizi di questa mafia virtuale in cambio di denaro.
Quindi può accadere che se lavorate come progettista e vendete i vostri progetti su Second Life, potreste vedere tutti i vostri lavori rubati e venduti da qualcun altro in qualche altro angolo di Second Life.
In tal caso potete bloccare questo criminale chiedendo a Second Life di bannare[10] (estromettere) il ladro dalla comunità virtuale, e quindi denunciarlo per violazione di copyright[11]. Ad ogni modo, in casi del genere la difficoltà principale sta nel scoprire il crimine e chi lo perpetra, visto che Second Life è composta da circa 8 milioni di utenti e la community continua a crescere. Questo significa che è realmente difficile rendersi conto quando qualcun altro cerca di arricchirsi grazie al vostro lavoro e chi esso sia. Purtroppo lo sfruttamento delle idee e del lavoro altrui non è l'unico problema nel mondo virtuale. Il furto di identità è un'altra disavventura in cui è possibile incorrere. Infatti, un blogger[12] ha descritto ciò che è accaduto ad un utente di Second Life, il quale è stato truffato in una trattativa di compravendita di immobili da qualcuno che aveva rubato l'identità di un altro utente per effettuare una transazione Pay-Pal[13].
Ma cerchiamo di analizzare un po' più nel dettaglio le varie tipologie di truffe nel mondo virtuale, basandoci su quanto si è potuto scoprire fino ad ora, non essendoci nel mondo di Second Life nessuna possibilità di avere un controllo reale e totale su ciò che accade in questo mondo parallelo.

Piramide:

Si tratta di un oggetto a forma di piramide che si trova un po' ovunque ed è riconoscibile dalla riproduzione di una banconota e da un testo che dice "toccami per fare soldi" ("touch me to make money"). Questo oggetto è

conosciuto anche come piramide truffa (Pyramid Scam) perché si affida sul fatto che altri acquistino il tuo oggetto che a loro volta dovranno piazzare in un luogo con un effetto piramidale che ricorda le Catene di S' Antonio.

Eliminazioni:

In Second Life nessuno può eliminare/uccidere un residente, si può "morire" solo se si partecipa a dei combattimenti nelle apposite aree che sono sempre indicate. Purtroppo, però, non tutti i videogiocatori di Second Life conoscono questa regola e vi sono dei "furbetti"che approfittano di questa mancata conoscenza per guadagnare soldi facili. Il meccanismo è molto semplice: un avatar minaccia un altro di ucciderlo se non pagherà una determinata somma di denaro, questo ignaro dell'impossibilità di essere ucciso e preoccupato dal fatto che potrebbe perdere tutto ciò che ha costruito fino a quel momento accetta e paga il truffatore.

Continue molestie:

Molti residenti non sanno che se ritengono di essere vittima di insulti o danneggiamenti da parte di un altro avatar è possibile redigere un rapporto di abuso ed è anche possibile zittire il molestatore o tele-trasportare il proprio personaggio in un'altra area ed eliminare il problema. Questo ignorare tale opportunità spinge molti giocatori ad accettare il ricatto imposto dal molestatore, il quale chiede dei soldi per smettere di infastidire o insultare la povera vittima.

Truffa del venditore invisibile**:**

In Second Life esiste la possibilità di creare oggetti invisibili/trasparenti, ma esiste anche la possibilità, attraverso un determinato comando, di vedere tali oggetti, che appaiono circondati da un alone rosso. I truffatori cercano di sfruttare gli oggetti invisibili sistemandoli sopra a venditori automatici, così

che ad essere pagato per l'acquisto non è il legittimo venditore ma il truffatore.

Vendite di oggetti falsificati:

Questa truffa riguarda un'immagine, o una tessitura, posta sopra un venditore automatico, che nasconde l'oggetto reale in vendita. In questo modo l'acquirente è convinto di acquistare l'oggetto che desidera ma in realtà non è così.

Sconti falsificati:

Vi sono dei truffatori che avvicinano le vittime all'interno dei negozi proponendo loro degli sconti sulla merce, ma solo se l'ignaro acquirente compra direttamente da lui, spacciandosi per il proprietario del negozio o per un importante socio. In realtà non vi sarà nessuno sconto e non v sarà neppure la merce.

Carte di credito:

Figura 10: Carta di credito di Second Life

La FirtMeta, fornitore di servizi finanziari per il mondo digitale, lancia la prima carta di credito virtuale MetaCard, utilizzabile in Second Life così

come si utilizzata la classica carta di credito nel mondo reale, la MetaCard sarà di due tipi: Basi e Gold.
La Basic card sarà soggetta al controllo dell'avatar e ha un massimo di credito di L$5000 (pari a circa $18.60) al mese, mentre la versione Gold offrirà un tetto massimo di credito di L$10,000 ($37.20) al mese e potrà essere rilasciata solo in seguito del rilascio delle credenziali della vera carta di credito ossia posseduta nella vita vera.
Adesso non resta da chiedersi se la prima carte di credito virtuale avrà gli stessi problemi di quella reale: ossia il rischio clonazione. Il quale non dovrebbe presentare particolari difficoltà per i cyber truffatori, per i quali basterà scrivere stando comodamente a casa appositi codici maligni per rubare dati e numeri di conto degli ignari utenti di Second Life, ma per fortuna questa resta per ora soltanto un ipotesi.

Truffe bancarie:

Ci sono molte banche in Second Life , alcune offrono tassi di interesse ridicolmente alti per catturare più avatar possibili, salvo poi accorgersi che il tasso di interesse è crollato e che ci sono spese da pagare o scoprire che non è più possibile accedere ai propri risparmi come è accaduto con il caso della Banca d'Italia SL e di Ginko Financial.
Non sono gli unici casi in cui il sistema economico di Second Life viene colpito da problemi che si ripercuotono sul reale. A fine luglio 2007 venne segnalato il furto di 12 mila dollari reali da parte di un ex dipendente della borsa Stock Exchange, perpetrato tramite la rete di bancomat virtuale di Second Life.
Second Life però sta cercando di evitare che casi come questi accadano ancora, infatti dal 22 gennaio 2008 Linden Lab ha deciso di non tollerare più e di chiudere quegli "istituti" che non hanno presentato una certificazione governativa valida o il benestare di un istituto finanziario reale. Ovviamente Linden Lab vieta, ma non controlla, non avendone i

mezzi, invita però a segnalare eventuali violazioni della disposizione suddetta.

Il Caso Banca D'Italia Second Life:

Banca d'ItaliaSL è la prima Banca Italiana nel mondo di Second Life.
La Banca ha iniziato ufficialmente la sua attività il giorno 16 Aprile 2007 per poi terminare verso la fine dell'anno 2007. La banca si è presentata come un solido istituto operativo sotto ogni punto di vista, con diversi tipi di azioni possibili:
depositare i propri risparmi, avere interessi giornalieri molto competitivi, prelevare denaro, il sistema Lotteria e Giochi attivo ecc. ecc.
I tassi offerti dalla banca erano i seguenti :
da 1 a 4999 L$ versati 0.20% di interessi giornalieri
da 5000 a 9999 L$ versati 0.25% di interessi giornalieri
da 10000 L$ in su 0.30% giornalieri
Improvvisamente la Banca d'Italia SL ha iniziato ad avere dei seri problemi, tanto che è stato istituito un gruppo nominato appunto: "Problemi Banca d'Italia SL" per cercare di capire l'evolversi e le possibili conseguenze di tale situazione. L'unica certezza che gli abitanti di Second Life hanno è che dal giorno in cui è nata Banca d'Italia al 28 Novembre 2007 le procedure di prelevamento hanno funzionato regolarmente, successivamente però i soldi non venivano più incassati.
Inizialmente si è pensato fosse un fastidioso problema di mancanza momentanea di fondi nell'account dell'istituto, purtroppo però non è stato così, bensì si è rivelato essere un vero e proprio crack finanziario simile a quello avvenuto precedentemente alla "Ginko Financial" (banca australiana grazie alla quale molti utenti hanno perso diversi dollari reali).
Le attività finanziarie in Second Life sono giustamente ritenute dagli esperti esercizi estremamente rischiosi, in quanto si è in un contesto privo di regole, infatti le norme della vita reale non sono e non possono essere applicate in un contesto che si autodefinisce ludico e dove per primi i promotori di tali

servizi precisano che si tratta solo di un gioco di ruolo e che, di conseguenza non vi possono essere delle garanzie. Anche la Banca d'Italia SL avvisò di questa assenza di garanzia i propri utenti con il seguente comunicato:
"Gli account non sono assicurati in nessun modo da nessun governo, come nel caso di molti conti correnti nella vita reale, così anche noi non possiamo garantire di non andare mai in bancarotta. Certamente Banca d'Italia SL non vuole questo e ci impegneremo per poter garantire un'istituzione sempre solida e affidabile, ma è corretto e onesto essere consapevoli dei rischi appena descritti." A carico di Banca d'Italia SL vi fu, in precedenza, anche un altro episodio alquanto sospetto, infatti nell'agosto del 2007 il servizio di sicurezza della vera Banca d'Italia ha scoperto nella rete la presenza dei portali www.bancaditalia.com e www.bancaditaliasl.altervista.org le cui denominazioni e i cui loghi richiamavano apertamente la Banca d'Italia e il suo sito. Per questo motivo la vera Banca d'Italia decise di segnalare tali irregolarità alle autorità competenti. Il forte sospetto è che si possa essere trattato di un caso di phishing o quanto meno di sfruttamento abusivo del marchio.

Testimonianza di un utente truffato in Second Life:

Di seguito propongo una testimonianza avuta via mail da un utente di Second Life che, sfortunatamente è stato truffato da un "collega".

> "Nell'estate del 2007 acquistai una parcel (terreno virtuale) dove mettere una piccola casetta per me ed un negozio dove poter vendere i miei articoli. Dopo qualche tempo, si traferì vicino alla mia parcel un altro avatar (utente,personaggio) di nome Luigeddu Arbizu.
> Sul suo terreno in breve creò un club con tanto di Escort Virtuali, di cui Second Life è piena. Ci conoscemmo poco dopo a causa di un vicino comune che disturbava con le sue costruzioni i nostri terreni.
> Luigeddu si presentò come un italiano, traferitosi prima a Londra e poi a Barcellona per lavorare come cameriere.

Dopo qualche tempo, decisi di vendere quel terreno e lo contattai per sapere se fosse interessato. A quel punto mi propose di metterci in società, comprare altri terreni virtuali e allestire un club. Accettai.

Fondò cosi un gruppo, dove entrambi eravamo i proprietari, a cui deedare[14](intestare) i terreni acquistati. In breve arrivammo a possedere più di 16mila metri di terreno, divisi equamente fra me e lui. Se non ricordo male, lui era al 55% e io al 45%, quindi una differenza minima. Tramite la fondazione di questo gruppo, l'uno poteva agire (costruendo o modificando) sul terreno dell'altro. Allo stesso tempo, gli introiti sarebbero stati divisi.

La costruzione del club continuò per circa un mese, successivamente, nell'ottobre 2007 decidemmo di aprire ufficialmente con una festa. La festa durò fino alle 2 di notte, dopodiché andai a dormire. Luigeddu però rimase connesso...

...il giorno dopo mi collegai di buon mattino e ricevetti l'avviso di return (cioè tutti i miei oggetti presenti sul terreno erano stati tolti). Mi fiondai a controllare il club e non lo trovai più. Notai che i 16mila metri totali erano stati suddivisi in metrature più piccole e vendute a ignari acquirenti. Contattai subito a Luigeddu, sia su msn messenger che su Second Life. Non in linea.

Controllai meglio e vidi che era stato già venduto l'80% dei terreni. E io da quella vendita non avevo ricevuto un Linden. Contattai i nuovi proprietari, vari americani, che mi spiegarono che verso le 4 del mattino si erano imbattuti in questi terreni proposti a prezzi particolarmente bassi. Finalmente Luigeddu si collegò. Nel chiedergli spiegazioni,lui non rispose. Gli chiesi la mia parte di denaro e in maniera poco carina mi scrisse “Wow!! ho 100.000 LINDEN (380 dollari circa) in più e non te li do”.

Contattai di nuovo i nuovi proprietari,spiegando del raggiro e chiedendo la restituzione dei terreni. Rifiutarono. Contattai la Linden Lab (la società dietro second life) spiegando la situazione e allegando documentazioni come prove.

La risposta: “Ci dispiace e possiamo capire il tuo sconforto, ma noi non ci occupiamo e non interveniamo su ciò che capita fra i residenti”.
Tornai quindi su Second Life e rezzai (costruire in Second Life) un enorme cartellone con scritto “NON COMPRATE TERRENI RUBATI DA LUIGEDDU ARBIZU” sopra i miei ormai ex-terreni. Ricevetti qualche messaggio di conforto dai residenti li vicino, ma nel giro di qualche giorno li ritrovai come proprietari degli ultimi terreni in vendita.
Il procedimento usato da Luigeddu è stato quindi questo:
-propormi un'attività in comune
-creare un gruppo a cui intestare i miei e suoi terreni, facendomi quindi fidare di lui
-agire sui miei terreni intestati al gruppo rivendendoseli a se stesso per 0 Linden
-rivendere i terreni a prezzi bassissimi per liberarsene subito.
Dal punto di vista della mia tutela la società proprietaria di Second Life non ha mosso un dito (questo avatar è ancora in circolazione) mentre contattando conoscenti nella Polizia Postale, pur essendo io in possesso del suo nome reale, mi è stato detto che non era accusabile di nulla.”

Il bug di Quick Time:[15]

Non solo in Second Life si può rimanere vittime di truffe dovute alla mancanza di regole e al comportamento scorretto tenuto dagli utenti, si può anche essere truffati a causa di una lacuna nel sistema di sicurezza del noto programma di Apple: Quick Time.
Il bug è causato dall'errata gestione degli header[16] mal formattati da parte del gestore del protocollo Real Time Streaming Protocol (RTSP)[17]: la ricezione di un pacchetto, opportunamente modificato, causa nel computer client un buffer overflow[18], sfruttabile dall'attacker per eseguire codice

binario a proprio piacimento. Il motivo per cui gli utenti di Second Life potrebbe subire delle truffe a causa di mancanza di Quick Time è semplice da spiegare: molti utenti di Second Life, quando costruiscono le loro case virtuali, i centri shopping digitali e tutte le altre strutture composte di bit che rendono "abitabile" la seconda vita, utilizzano proprio QuickTime. Lo usano come sistema per mostrare video all'interno di Second Life e per "arredare" i loro spazi virtuali. Il problema è che a causa di questo falla nel sistema c'è chi riesce ad approfittarsi della vulnerabilità di QuickTime per far passare altre informazioni digitali che hanno un effetto paradossale. Permettono cioè di borseggiare gli avatar che si avvicinano troppo ai video incriminati e sfilargli metaforicamente il portafoglio digitale di tasca, dove ci sono i Linden dollars, cioè la valuta virtuale che però è convertibile in dollari veri. C'è un caso citato anche dalla stampa americana di due esperti di sicurezza, Charlie Miller e Dino Dai Zovi, che, con l'intento di dimostrare la pericolosità di questo bug, sono riusciti a creare un codice capace di estrarre ben 12 Linden dollars (pari più o meno a quattro centesimi e mezzo di dollari veri) dagli avatar che si trovano nelle vicinanze del video incriminato. In pratica, nel meta mondo, ci si può trovare di fronte a oggetti o gadget che riproducono video utilizzando il player Quick Time. Per mostrare il video, il software si connette ad un server remoto che non fa parte di Second Life: un server creato ad hoc, che può permettere a un malintenzionato di prendere il controllo dell'avatar della vittima. Basta che l'avatar del personaggio si avvicini al "gadget minaccia", per rimanere truffato. Inoltre, nel momento in cui si viene attaccati, per alcuni secondi si perde il controllo del proprio personaggio. Quindi è sufficiente andarsene a spasso in giro per restare truffati: qualunque oggetto potrebbe caricare un filmato "maligno". Purtroppo anche in questo caso nessun residente di Second Life verrà tutelato infatti, finché Apple (produttore di QuickTime) non troverà una soluzione, Second Life ha fatto sapere che non risarcirà gli utenti vittima dei "borseggi".

Capitolo 6: Conclusioni

Dopo aver analizzato le truffe, sia del mondo reale che del mondo virtuale di Second Life, si può notare come vi siano degli elementi e delle caratteristiche che si possono ritrovare in quasi tutte le varie tipologie di truffa. A questo punto diventa possibile pensare che si possa informatizzare la struttura base delle truffe.
La tecnologia informatica che meglio si adatta a un lavoro di questo tipo è sicuramente l'XML.

6.01. Cos'è l'XML?

L'XML, acronimo di eXtensible Markup Language, ovvero "Linguaggio di marcatura estensibile" è un metalinguaggio creato e gestito dal World Wide Web Consortium (W3C). XML è dunque un meta-linguaggio per definire la struttura di documenti e dati. Il termine documento ricorre spesso nella terminologia XML. Anche se esso può far pensare pagine Web o altri prodotti dell'elaborazione di testo, è utilizzato nella sua accezione più ampia di contenitore di informazioni.
Concretamente, un documento XML è un file di testo che contiene una serie di tag, attributi e testo secondo regole sintattiche ben definite.
Analizziamo ora XML dal punto di vista logico e sintattico e i documenti che con esso si possono creare dando uno sguardo alla struttura logica. Introduciamo alcuni concetti fondamentali per la corretta comprensione di questo meta-linguaggio. Un documento XML è intrinsecamente caratterizzato da una struttura gerarchica. Esso è composto da componenti denominati elementi. Ciascun elemento rappresenta un componente logico del documento e può contenere altri elementi (sottoelementi) o del testo. Gli elementi possono avere associate altre informazioni che ne descrivono le proprietà. Queste informazioni sono chiamate attributi.
L'organizzazione degli elementi segue un ordine gerarchico o arboreo che prevede un elemento principale, chiamato root element o semplicemente

root o radice. La radice contiene l'insieme degli altri elementi del documento. La struttura logica di un documento XML viene tradotta in una corrispondente struttura fisica composta di elementi sintattici chiamati tag**.** Questa struttura fisica viene implementata tramite un file di testo creato con un qualsiasi editor.

6.02 Descrizione di una truffa realmente accaduta.

Tipologia della truffa: falsa beneficenza:

Savona, Marzo 2005.
Ore 14:30, un distinto signore italiano di circa quarant'anni passeggia per il centro città con aria tranquilla. Con disinvoltura avvicina un'anziana signora, i due iniziano a parlare del più e del meno, come si usa dire, nel dialogar l'uomo racconta alla donna di essere un importante dottore. Durante la conversazione sopraggiunge un'automobile, dalla quale scende un giovane uomo (complice del finto medico) in cerca di informazioni. Il giovane sostiene di essere svizzero e di essere in Italia per consegnare una donazione a una famosa associazione umanitaria di un noto dottore.
Il finto dottore si finge interessato e, davanti all'anziana signora, chiede maggiori informazioni riguardanti l'associazione e il famoso medico.
Parlando si scopre che il finto dottore conosce il collega dell'associazione, ma che purtroppo l'uomo era deceduto da pochi giorni. Il ragazzo svizzero si fine addolorato e, allo stesso tempo, preoccupato perché ora vi era il rischio che la donazione andasse persa e che i poveri pazienti del medico, facente parte dell'associazione, non avrebbero potuto ottenere i costosi macchinari a cui erano destinati i soldi recuperati dall'asta di beneficenza organizzata il mese precedente. A questo punto i due malfattori chiedono all'anziana signora, la quale ha assistito all'intera scena, se avrebbe potuto gentilmente aiutarli a consegnare, comunque, la somma di denaro.
La signora davanti alla richiesta di aiuto per portare a termine un opera buona non può far altro che accettare e mettersi a disposizione dei due

truffatori. La prima richiesta di aiuto fatta all'anziana donna consiste nell'accompagnare il finto medico e giovane da un notaio della città. Durante il tragitto il giovane si accorge che al notaio andranno sicuramente anticipati dei soldi, indicativamente tre mila / quattro mila euro. Entrambi dichiarano di non essere in possesso di tale somma e chiedono alla signora se è disposta ad anticipare lei la piccola somma, rassicurandola che sarà in breve tempo rimborsata e che le sarà anche data una ricompensa direttamente dall'associazione umanitaria.

La donna viene, quindi, accompagnata in banca o a casa per prelevare la somma stabilita; mentre i tre individui si stanno recando dal notaio, il finto dottore informa il giovane e l'anziana signora che molto probabilmente dal notaio servirà anche una marca da bollo. Insieme si dirigono, dunque, da un tabaccaio, con una scusa i due convincono la donna a scendere dall'auto e ad andare a comprare la marca da bollo. Come l'anziana signora entra in tabaccheria i due truffatori si dileguano con i soldi della povera vittima.

6.03 Analisi della truffa attraverso l'editor VXE 2.2

<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<Descrizione - truffa - falsa - beneficenza>
<Dove>Savona</Dove>
<Quando>Marzo 2005. Ore 14:30</Quando>
<Chi - truffatore>un distinto signore italiano di circa quarant'anni</Chi - truffatore>
passeggia per il centro città con aria tranquilla. Con disinvoltura avvicina
<Chi - vittima>un'anziana signora</Chi - vittima>
i due iniziano a parlare del più e del meno, come si usa dire, nel dialogare l'uomo racconta alla donna di essere un importante dottore. Durante la conversazione sopraggiunge un'automobile, dalla quale scende
<Chi - complice>un giovane uomo in cerca di informazioni. Il giovane sostiene di essere svizzero</Chi - complice>
e di essere in Italia per

<Pretesto>consegnare una donazione a una famosa associazione umanitaria di un noto dottore.</Pretesto>

Il finto dottore si finge interessato e, davanti all'anziana signora, chiede maggiori informazioni riguardanti l'associazione e il famoso medico. Parlando si scopre che il finto dottore conosce il collega dell'associazione, ma che purtroppo

<Problema>il famoso dottore dell'associazione umanitaria era deceduto da pochi giorni.</Problema>

Il ragazzo svizzero si fine addolorato e, allo stesso tempo, preoccupato perché

<Problema-2>ora vi era il rischio che la donazione andasse persa e che i poveri pazienti del medico, facente parte dell'associazione, non avrebbero potuto ottenere i costosi macchinari a cui erano destinati i soldi recuperati dall'asta di beneficenza organizzata il mese precedente</Problema-2>

A questo punto i due malfattori chiedono all'anziana signora, la quale ha assistito all'intera scena, se avrebbe potuto gentilmente aiutarli a consegnare, comunque, la somma di denaro. La signora davanti alla richiesta di aiuto per portare a termine un opera buona non può far altro che accettare e mettersi a disposizione dei due truffatori.

<Prima – richiesta – di - aiuto>La prima richiesta di aiuto fatta all'anziana donna consiste nell'accompagnare i due truffatori da un notaio della città.</Prima - richiesta - di - aiuto>

Durante il tragitto il giovane si accorge che al notaio andranno sicuramente anticipati dei soldi, indicativamente tre mila / quattro mila euro. Entrambi dichiarano di non essere in possesso di tale somma

<Seconda - richiesta - di - aiuto>chiedono alla signora se è disposta ad anticipare lei la somma di denaro per il notaio, rassicurandola che sarà in breve tempo rimborsata e che le sarà anche data una ricompensa direttamente dall'associazione umanitaria.</Seconda – richiesta – di - aiuto>

La donna viene, quindi, accompagnata in banca o a casa per prelevare la somma stabilita; mentre i tre individui si stanno recando dal notaio, il finto dottore informa il giovane e l'anziana signora che molto probabilmente dal

notaio servirà anche una marca da bollo. Insieme si dirigono, dunque, da un tabaccaio, con una scusa

<Terza - richiesta – di - aiuto>i due convincono la donna a scendere dall'auto e ad andare a comprare la marca da bollo.</Terza – richiesta – di - aiuto>

<Epilogo>Come l'anziana signora entra in tabaccheria i due truffatori si dileguano con i soldi della povera vittima</Epilogo>

</Descrizione - truffa - falsa - beneficenza>

6.04 Albero degli elementi

Descrizione truffa falsa beneficenza

- Dove
- Quando
- Chi truffatore
- Chi vittima
- Chi complice
- Pretesto
- Problema
- Problema 2
- Prima richiesta di aiuto
- Seconde richiesta di aiuto
- Terza richiesta di aiuto
- Epilogo

RINGRAZIAMENTI

Desidero ringraziare il Professor Giovanni Degli Antoni per avermi proposto per la mia tesi questo interessante argomento, per aver dimostrato fiducia in me e nelle mie capacità tanto da avermi lasciato la "libertà" di organizzare questo lavoro come meglio credevo senza mai impormi nulla, ma sostenendomi con preziosi insegnamenti e consigli.

NOTE

Nota **1** :
Fondata a Roma nel 1971, la Confesercenti è una delle principali associazioni delle imprese in Italia. (http://www.confesercenti.it/).

Nota **2**:
Tratto da Confesercenti, lo studio completo lo si può trovare all'indirizzo: http://www.confesercenti.it/documenti/allegati/2006truffe.doc

Nota **3** :
Frank William Abagnale Jr. (New Rochelle, New York, USA, 27 aprile 1948) è stato un truffatore attivo per cinque anni durante gli anni '60. È successivamente diventato consulente finanziario specializzato nel contrasto delle truffe finanziarie.

Nota **4**:
Tratto da Antolisei, Manuale di diritto penale

Nota **5** :
Paolo Attivissimo,giornalista, scrittore, creatore e autore del Servizio Antibufala (http://antibufala.info) dedicato alle indagini sugli appelli, gli allarmi e le dicerie che girano in Rete), del blog informatico Il Disinformatico (http://disinformatico.info) e della newsletter "Internet per tutti".

Nota **6**:
La Linden Research, Inc è la software house che ha sviluppato il popolare gioco Second Life. La Linden Lab è stata fondata nel 1999 da Philip Rosedale allo scopo di realizzare ambienti virtuali. http://lindenlab.com/

Nota **7**:
Il Dollaro Linden o Linden Dollar è la moneta di scambio usata nell'economia del mondo virtuale di Second Life.

Con i Dollari Linden in Second Life si può acquistare e vendere terreni e oggetti e possono essere riconvertiti in denaro reale. . Nel 2006 il cambio del Linden Dollar variava da L$260/USD a L$320/USD.
2008 1 Euro corrisponde a 330 Linden Dollars, 1 Dollaro USA a 285 Linden Dollars

Nota **8**:
Un cyber criminale è colui che pratica e promuove attività criminose attraverso l'uso di Internet

Nota **9**:
Visual Studio è un ambiente di sviluppo integrato sviluppato da Microsoft, che supporta diversi tipi di linguaggio e che permette la realizzazione di siti web, applicazioni web e servizi web.

Nota **10**:
Bannare: letteralmente: proibire/impedire. Bannare un utente da un forum, o da un qualsiasi luogo virtuale, significa impedire che questa persona possa accedere al "luogo". E' un provvedimento estremo applicato dall'amministratore qualora l'utente violasse ripetutamente le regole della netiquette.(insieme di regole che disciplinano il comportamento di un utente di Internet nel rapportarsi agli altri utenti).

Nota **11**:
Copyright: diritto che tutela la proprietà di un'opera letteraria, musicale, ecc. e ne impedisce la riproduzione abusiva

Nota **12**:
Blogger: il creatore e curatore di un blog (un diario in rete.).

Nota **13**:
Paypal è uno strumento di micro - pagamento utilizzato nell'e-commerce, tramite il quale è possibile effettuare transazioni presso molti negozi online

Nota **14** :
Deedare dal verbo to deed, che può essere inteso come donare o intestare

Nota **15**:

QuickTime è il nome che Apple Inc. ha dato all'architettura del suo sottosistema di visualizzazione e al suo formato di file proprietario molto diffuso su sistemi Macintosh

Nota **16**:

Header: è l'intestazione della "busta" dei dati trasmessi, quella parte del pacchetto che precede i dati veri e propri e che indica la fonte, la destinazione e le informazioni sul controllo degli errori che, nel tragitto, si potrebbero verificare.

Nota **17**:

Il protocollo RTSP è stato sviluppato da RealNetworks, Netscape Communications, e Columbia University. L'RTSP ottimizza il flusso di dati

Nota **18**:

Il buffer overflow è una vulnerabilità di sicurezza che può affliggere un programma software. Consiste nel fatto che tale programma non controlla in anticipo la lunghezza dei dati in arrivo, ma si limita a scrivere il loro valore in un buffer di lunghezza prestabilita, confidando che l'utente (o il mittente) non immetta più dati di quanti esso ne possa contenere: questo può accadere se il programma è stato scritto usando funzioni di libreria di input/output che non fanno controlli sulle dimensioni dei dati trasferiti.

BIBLIOGRAFIA

Antolisei F, "Manuale di diritto penale", Giuffrè, Milano, 1987

Bardi D., "Dalla matita rossa e blu alla struttura dei testi. Suggerimenti da XML ", La scuola, Milano, 2005

Biggs J. , "Black Hat. Crimini, misfatti e truffe sul Web", Mondadori Informatica, 2004

Lessig L. "Code and other laws of cyberspace", Basic book, 2006

FILMOGRAFIA

Foley J. "Confidence", Burns M., Buton M, Ohven M., Usa, Canada, Germania, 2003

Hill G.R. "La stangata", Philips B. Usa, 1973

Scott R. "Il genio della truffa", Bailey S., Griffin T., Rapke J., Scott R., Storkey S., Zemeckis R., Usa 2003

Spielberg S. "Prova a prendermi", Parkes W.F., Spielberg S., Usa, 2002

SITI WEB

Cmap Tools: http://cmap.ihmc.us/conceptmap.html

Confesercenti: http://www.confesercenti.it/

Gaia Rossini: http://gaiarossini.myblog.it/sl_truffe_-_/

Il disinformatico: http://attivissimo.blogspot.com/2004_06_01_archive.html

Il truffato: http://www.truffato.com/forum/

Linden Lab: http://lindenlab.com/

Nova multimedia: http://www.nova-multimedia.it

Polizia di stato: http://www.poliziadistato.it

Second Life: http://wiki.secondlife.com/

Second Life Italia: http://www.secondlifeitalia.com/wiki/Truffe

Wikipedia: http://www.wikipedia.com

Xml per tutti: http://www.xmlpertutti.com

PROGRAMMI

Visual XML Editor VXE 2.2

Editor attraverso il quale è possibile:
Gestire, creare, pubblicare il proprio podcast
Visualizzare graficamente i nodi XML in una mappa interattiva
Formattare più correttamente i documenti generati html
VXE 2.2 presenta una successione di strumenti per lo sviluppo di Xdidattica,progetto di collaborazione tra l'Università degli Studi di Milano e il liceo Scientifico "Lussana" di Bergamo. Il progetto Xdidattica è diretto da G. Degli Antoni e da D. Baldi.

CmapTools version 4.16

CmapTools è un software multipiattaforma per sviluppare, navigare, condividere mappe concettuali, realizzato dall'Institute for Human and Machine Cognition dell'università della West Florida.

FIGURE

FIGURA 1: ESEMPIO PHISHING BANCA INTESA. 23
FIGURA 2: ESEMPIO PHISHING POSTE ITALIANE 24
FIGURA 3: LOCANDINA CONFIDENCE. 30
FIGURA 4: LOCANDINA PROVA A PRENDERMI. 33
FIGURA 5: FRANK W. ABAGNALE. 33
FIGURA 6: LOCANDINA LA STANGATA 35
FIGURA 7: LOCANDINA IL GENIO DELLA TRUFFA. 37
FIGURA 8: LOGO SECOND LIFE. 39
FIGURA 9: IMMAGINI SECOND LIFE. 40
FIGURA 10: CARTE DI CREDITO SECOND LIFE 44