# LA SICUREZZA NELLE COMUNICAZIONI TELEMATICHE: UN OBIETTIVO DI QUALITÀ NECESSARIO

**Vito Santarcangelo[1°], Nancy Santarcangelo[2]**

*[1] Centro Studi S.r.l. , Zona Industriale Loc. Sant'Antuono - 84035 Polla (SA)*
*[2] BNG S.r.l. – Via Ravenna, 2 - 75015 Ferrandina (MT)*
*° autore di riferimento - email: info@iinformatica.it*

***Riassunto***

*Il lavoro offre una panoramica sullo spoofing (falsificazione di identità), tematica di notevole attualità, riguardante le comunicazioni telematiche. Telefonate, fax, sms e e-mail sono i principali mezzi utilizzati dalla Social Engineering (ingegneria sociale) per compiere azioni illecite. L'obiettivo del lavoro è di contribuire alla conoscenza del fenomeno e presentare protocolli comportamentali e strumenti da utilizzare per difendersene.*

## 1. INTRODUZIONE

Il filosofo greco Aristotele (IV sec. a. C.) scrisse nella sua Politica, *"l'uomo è un animale sociale": tende per natura ad aggregarsi con altri individui e a costituirsi in società*. Questa necessità ha facilitato lo sviluppo e una più facile diffusione delle comunicazioni telematiche, che unificando metodologie e tecniche delle telecomunicazioni e dell'informatica hanno permesso di realizzare il trasferimento a distanza delle informazioni e delle elaborazioni di qualsiasi tipo di dato.

Le comunicazioni telematiche sono ormai insite all'interno dei nostri comportamenti, e caratterizzano parte della nostra quotidianità. Mandare o leggere una mail, telefonare, inviare un messaggio è ormai un'azione comune alla moltitudine e diventa sempre più necessaria per eliminare la barriera della distanza fisica.

La risposta del progresso a tale necessità è stata la realizzazione di "Social Network", consolidatesi sempre di più grazie all'uso ormai comune e diffuso della rete Internet.

Se queste forme di aggregazione telematica possono influenzare positivamente la vita sociale, si pensi alla possibilità di conoscere persone e culture diverse rimanendosene comodamente a casa, alla possibilità di ricercare personale e profili professionali ad hoc su larga scala, studiare fenomeni culturali con l'ausilio di qualche click, possono, nello stesso tempo, comportare notevoli rischi di utilizzazione. .

Primo fra tutti, per le relative conseguenze che potrebbero scaturirne, è l'utilizzo di false identità. Nessuno di noi può conoscere effettivamente la vera identità dell'interlocutore attraverso un canale telematico(sia sms, telefono, e-mail o canali internet), almeno inizialmente.

Lo scopo di questo lavoro è proprio quello di far conoscere le principali modalità di falsificazione dell'identità e proporre protocolli comportamentali o strumenti da utilizzare per difendersi da esse.

## 2. SPOOFING TELEMATICO: SMISHING, VISHING, PHISHING

Le tecniche di spoofing [1] (falsificazione di identità) possono essere relative a sms, telefonate e - mail. Si vuole con tale panoramica sensibilizzare il lettore sulla semplicità di mettere in atto tale tecnica di attacco.

Lo spoofing può riguardare i vari sistemi di comunicazione quali ad esempio messaggistica, telefonate, e-mail. La figura illustra in maniera semplice come agisce a livello logico la falsificazione di un pacchetto fra pc in rete. PC1 manda a PC3 un "insulto" fingendosi PC2, PC3 verifica il mittente e licenzia PC2.

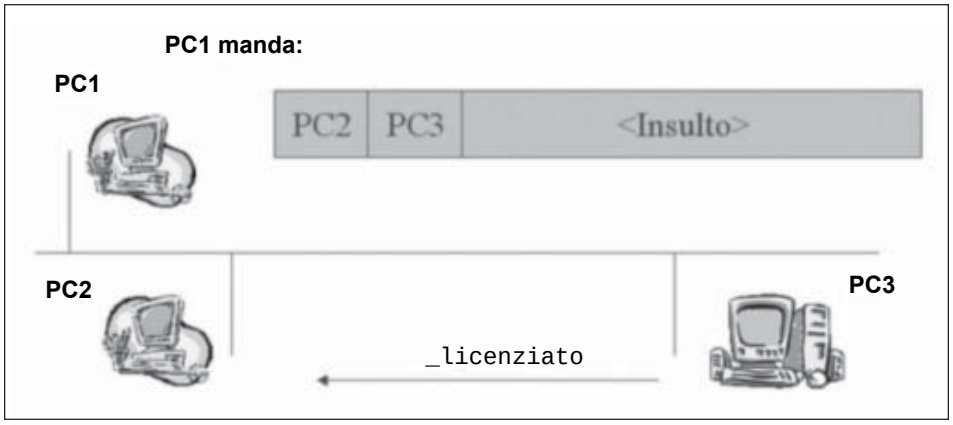


**Fig. 1: Esempio base di spoofing di un pacchetto [7]**

Lo smishing (spoofing SMS) consiste nell'utilizzare come mittente di un SMS un numero da noi prescelto, appropiandosi in questo modo di un'altra identità.

La tecnica di falsificazione di un SMS consiste per esempio nell'utilizzare il protocollo UCP (Universal Computer Protocol).

In questo caso il pacchetto UCP è composto da una stringa di caratteri <STX>HEADER/DATA/CRC<EXT> dove <STX> è l'inizio del messaggio e <EXT> è la fine del messaggio. Lo spoofing semplicemente si attua impostando **il numero sorgente del messaggio (OadC)** nel campo DATA.

Il vishing è lo spoofing attraverso le telefonate. Ciò è possibile grazie alla commistione di rete VOIP (su rete IP) e rete tradizionale (PSTN). In questo caso è possibile impostare tramite centralino VOIP (es. Asterix) una qualsiasi identità (caller ID) ed effettuare uno spoofing di un numero di telefono [4].


**Fig. 2: Applicativo per smartphone per realizzare lo smishing**


**Fig. 3:**
**Applicativo per smartphone per realizzare il vishing**

Il telefono che riceverà la chiamata visualizzerà realmente il numero del chiamante spoofato, ci saremo appropriati anche in questo caso di una falsa identità. Servizi quali Kryptotel e Spoofcard permettono anche tramite l'utilizzo di semplici APP per Smartphone di poter effettuare lo spoofing di un numero desiderato, utilizzando addirittura l'ulteriore funzionalità di Voice Changer si può eventualmente modificare anche la voce.

L'e-mail spoofing consiste nell'inviare una qualsiasi e-mail con l'indirizzo di posta (mittente) da noi desiderato. In questo modo, solo conoscendo l'indirizzo e-mail della vittima, potremo sostituirci a lui senza destare il minimo dubbio in chi riceve l'e-mail stessa e senza lasciare traccia dell'invio nell'account di posta della vittima a cui abbiamo rubato l'identità.

Il mail spoofing si basa sull'assenza di autenticazione necessaria all'utilizzo del protocollo SMTP. Infatti è possibile inviare una mail dall'account info@iinformatica.it senza necessariamente autenticarsi con nome utente e password di tale casella di posta, ma utilizzando un altro SMTP come l'SMTP del gestore telefonico a cui si è connessi. Immaginiamo quindi di non essere i proprietari di tale casella di posta. Sfruttando tale tecnica è possibile inviare una mail da un account di cui non siamo i proprietari. La mail arriverà da info@iinformatica.it e per poter ottenere maggiori dettagli sull'smtp utilizzato è necessario studiare l'header della mail. Infatti, noi siamo abituati a visualizzare il solo body di una mail, in quanto il web client ci inibisce in automatico la visualizzazione dell'intestazione.

L'header della mail contiene, invece, tutte le informazioni utili per capire la storia della mail dall'invio alla ricezione. A tal proposito consideriamo un esempio di header mail proposto da Microsoft [6] della corrispondenza via mail fra Anton Kirilov avente mail anton@proseware.com e Kelly J. Weadock avente mail kelly@litwareinc.com.

Microsoft Mail Internet Headers Version 2.0
Received: from mail.litwareinc.com ([10.54.108.101]) by mail.proseware.com
with Microsoft SMTPSVC(6.0.3790.0);
Wed, 12 Dec 2007 13:39:22 -0800
Received: from mail ([10.54.108.23] RDNS failed) by mail.litware.com with
Microsoft SMTPSVC(6.0.3790.0);
Wed, 12 Dec 2007 13:38:49 -0800
From: "Kelly J. Weadock" <kelly@litware.com>
To: <anton@proseware.com>
Cc: <tim@cpandl.com>
Subject: Review of staff assignments

```
Date: Wed, 12 Dec 2007 13:38:31 -0800MIME-Version: 1.0
Content-Type: multipart/mixed;
X-Mailer: Microsoft Office Outlook, Build 12.0.4210
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+ipA= =
Return-Path: kelly@litware.com
Message-ID: <MAILbbnewS5TqCRL00000013@mail.litware.com>
X-OriginalArrivalTime: 12 Dec 2007 21:38:50.0145 (UTC)†
```

Di seguito si analizza l'header per parti.

1)

```
Received: from mail.litwareinc.com ([ 10.54.108.101]) by
mail.proseware.com with Microsoft SMTPSVC(6.0.3790.0);
Wed, 12 Dec 2007 13:39:22 -0800
Received: from mail ([ 10.54.108.23] RDNS failed) by mail.litware.com
with Microsoft SMTPSVC(6.0.3790.0);
Wed, 12 Dec 2007 13:38:49 -0800
```

Dall'header si evince la storia della mail, infatti alle ore 13:38:49 la mail è stata consegnata al server mail.litwareinc.com che consegna la mail alle ore 13:39:22 al server proseware prima di consegnarlo all'utente anton@proseware.com.

Inoltre, il trasferimento di questo messaggio è stato eseguito mercoledì 12 dicembre 2007, alle 13.39.22 ora solare Pacifico, ovvero 8 ore prima ("-0800") rispetto all'ora UTC (Coordinated Universal Time, Ora di Greenwich).

2)

```
From: "Kelly J. Weadock" <kelly@litware.com>
To: <anton@proseware.com>
Cc: <tim@cpandl.com>
Subject: Review of staff assignments
Date: Wed, 12 Dec 2007 13:38:31 -0800
```

Dall'header si evince il mittente e destinatario del messaggio e la persona che riceve il messaggio in copia per conoscenza (CC). Gli eventuali destinatari del messaggio in copia per conoscenza nascosta (Ccn) non sono leggibili nell'intestazione. Inoltre, vi è l'oggetto del messaggio di posta elettronica e la data e ora di effettivo invio del messaggio di posta elettronica, in base all'orologio del computer del mittente.

3)

```
X-Mailer: Microsoft Office Outlook, Build 12.0.4210
Thread-Index: AcON3CInEwkfLOQsQGeK8VCv3M+ipA==
```

Le informazioni indicano che questo messaggio è stato inviato utilizzando la versione build 12.0.4210 di Microsoft Office Outlook. Il thread-index è una intestazione utilizzata per associare più messaggi a un tema simile. Nella visualizzazione per conversazione di Outlook, ad esempio, queste informazioni vengono utilizzate per individuare i messaggi appartenenti allo stesso tema di conversazione.

L'email spoofing è il mezzo utilizzato per effettuare attacchi quali phishing o trojan-based. Il phishing è un tipo di truffa attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.

Un classico caso è quello della mail formale di un istituto bancario che invita all'inserimento delle proprie credenziali accedendo tramite un comodo link che rimanda ad una pagina fedelmente ricostruita del noto sito internet mediante l'utilizzo delle potenzialità offerte da javascript. Un attacco trojan-based [3] utilizza il mail spoofing per poter colonizzare il pc della vittima. Il trojan è solitamente nascosto dietro allegati allettanti per la vittima (fotografie, listini prezzi, ecc.).

Consideriamo, a titolo di esempio, il caso di un attaccante interessato ad accedere alla rete di una azienda di materassi di nome "Dormibene" dove dall'organigramma aziendale presente sul sito web ha evinto che il responsabile acquisti è la Sig.ra Rossella Fiducia.

L'attaccante conosce inoltre che il loro fornitore è la ditta "i3Lana" il cui responsabile acquisti è il Dott. Luca Vendobene (informazione evinta dal profilo Linkedin dello stesso). Nell'azienda "i3Lana" gli indirizzi e-mail sono strutturati nella forma inizialenome.cognome@i3lana.biz informazione ottenuta ricercando mail @i3lana.biz nei motori di ricerca.

Di conseguenza la mail del Dott. Vendobene sarà l.vendobene@i3lana.biz, di cui l'attaccante ha opportunamente verificato l'esistenza mediante i tool online di verifica e-mail. La Sig.ra Rossella Fiducia ha come mail rossella.fiducia@dormibene.com, indirizzo presente nel sito della ditta "Dormibene".

Il nostro attaccante per accedere alla rete aziendale invierà una mail a nome di Luca Vendobene effettuando il mail spoofing l.vendobene@i3lana.biz con un contenuto istituzionale ingannevole e un allegato allettante in modo da poter colonizzare il pc della vittima ed aver così accesso alle informazioni del pc della vittima e alla rete aziendale.

Con elevata probabilità la vittima, secondo il principio dell'ingegneria

sociale (di cui parleremo nel prossimo paragrafo) che asserisce che "Gli umani sono esseri molto fiduciosi nel prossimo e tendono a credere a ciò che si dice loro", aprirà l'allegato e se non appropriatamente protetto da un antivirus adeguato, il pc verrà colonizzato.

In caso di persona scettica potrebbe essere necessario combinare un attacco vishing in cui il Dott. Luca Vendobene annuncia l'arrivo della mail.

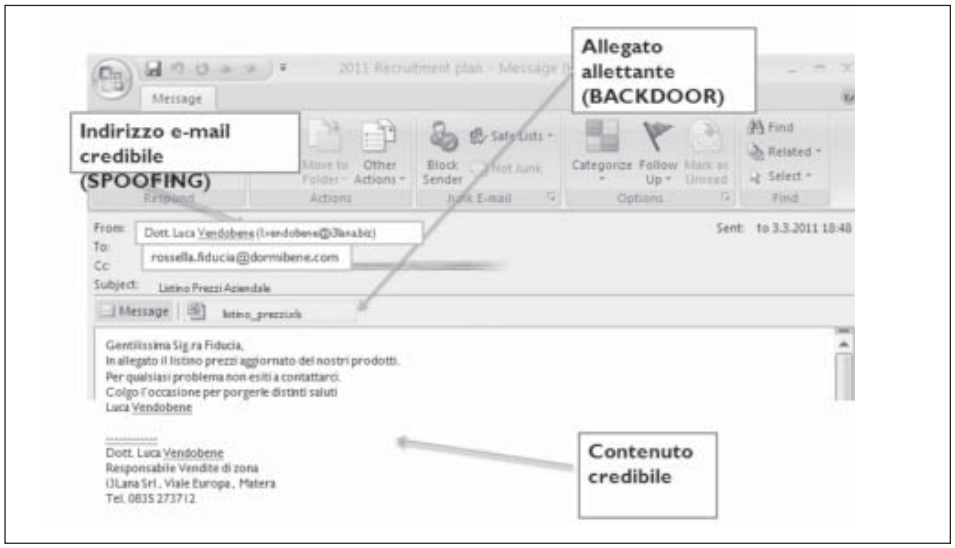


**Fig. 4: Esempio di mail spoofing con trojan [10]**

Consideriamo a tal proposito l'esempio dell'header mail spoofata da BOB.

Received: from **smtp.connessione.it**([82.XX.XXX.1XX]) by reicever.dormibene.com;
Fri, 6 Sep 2013 07:38:52 -0700
Received: from **pcBOB (79.5.XXX.XXX)** by **smtp.connessione.it** (8.XX.XXX.XX)
id 5224B1A202026606 for rossella.fiducia@dormibene.com;
Fri, 6 Sep 2013 16:38:50 +0200
Message-ID: <58A17E7F0D204AF2B16A74CBD5F938F5@**pcBOB**>
From: "Dott. Luca Vendobene" <l.vendobene@i3lana.biz>
To: <rossella.fiducia@dormibene.com>
Subject: Listino prezzi aggiornato
Date: Fri, 6 Sep 2013 16:38:55 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary=" - - - - =_NextPart_000_000E_01CEAB1F.9416C860"
X-Priority: 3
X-MSMail-Priority: Normal
**X-Mailer: Microsoft Outlook Express 6.00.2900.5931**
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.6157

Return-Path: l.vendobene@i3lana.biz
X-OriginalArrivalTime: 06 Sep 2013 14:38:52.0657 (UTC)

Nell'header si evince con facilità sia il riferimento dell'indirizzo ip pubblico da cui BOB ha inviato la mail , l'smtp server

della sua connessione utilizzato per effettuare lo spoofing e il client di posta utilizzato.

La pericolosità ed efficacia dello spoofing è notevole se pensiamo ad esempio al caso in cui vi sia una società di vigilanza che gestisca il piantonamento notturno di un cantiere e il cui protocollo di gestione giornaliera del piantonamento sia basato su invio mail. Un attaccante potrà effettuare mediante vishing la telefonata annunciando l'arrivo della mail spoofata che comunica la sospensione del servizio di piantonamento per quella sera con il conseguente lavoro semplificato per i malviventi.

Per arginare il problema del mail spoofing è tuttavia sufficiente utilizzare la **PEC** dove la veridicità della provenienza avviene mediante controllo della firma del gestore di posta pec (operazione effettuata in automatico dai principali client di posta).

Questo messaggio è firmato
– Il messaggio non è stato modificato
– Il certificato può essere verificato
– L'indirizzo email del mittente corrisponde al certificato contenuto nella email

**Fig. 5: Esempio di controllo automatico di una PEC ricevuta**

È importante perciò esigere sempre l'utilizzo delle mail PEC e verificarne l'autenticità del certificato, e cercare laddove possibile di avere un contatto diretto telefonico col personale.

## 3. INGEGNERIA SOCIALE E SOCIAL NETWORKS

Il termine «ingegneria sociale» (in inglese «social engineering») definisce l'arte di manipolare delle persone al fine di aggirare dei dispositivi di sicurezza [2]. E' una tecnica effettuata principalmente mediante comunicazioni telematiche (telefono, sms, e-mail,social network) ma gli stessi principi valgono per azioni effettuate per contatto diretto o posta tradizionale. Un ingegnere sociale (social engineer) "deve saper fingere, sapere ingannare gli altri, in una parola†saper mentire" [9]. La forza di persuasione dell'attaccan-

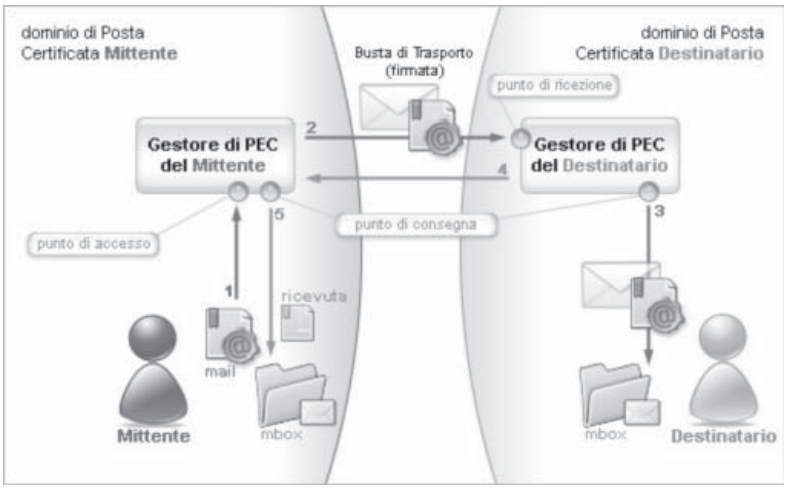


**Fig. 6: Schema della PEC illustrato da www.pec.it**

te e l'eccesso di fiducia da parte delle vittime sono i due cardini alla base dell'ingegneria sociale. Tutto parte dalla definizione dell'obiettivo e della relativa vittima. Vengono quindi ricercate le informazioni e riferimenti sulla vittima (questa è la fase di **footprinting** in cui le informazioni vengono reperite direttamente o mediante siti, motori di ricerca e social network) e reperite tali informazioni, esse vengono analizzate mediante la creazione di una mappa di analisi in cui ciascuna informazione viene pesata. Si definisce, così, un profilo della vittima mediante un **grafo sociale** (che lega persone e gruppi collegati alla vittima) e un **grafo degli interessi**.

Viene quindi definita la strategia da adottare per raggiungere l'obiettivo considerando le seguenti fasi:

- **fase iniziale** di approccio/fidelizzazione, per guadagnare la fiducia dell'utente, facendosi passare per una persona del suo gruppo, società, ambiente o per un cliente, un fornitore;
- **fase dell'attacco** con ottenimento delle informazioni obiettivo, tramite conversazione opportunamente pianificata oppure mediante l'invio di un avviso (es. pretesto di sicurezza o di una situazione di emergenza) o di materiale allettante con backdoor nascosta;
- **fase finale di invio di una diversione**, cioè una frase o una situazione che permetta di rassicurare l'utente evitando che si focalizzi sull'evento (conversazione/allegato). Può essere ad esempio un ringraziamento che annunci che tutto è rientrato nella norma nel caso di pretesto sicurezza/

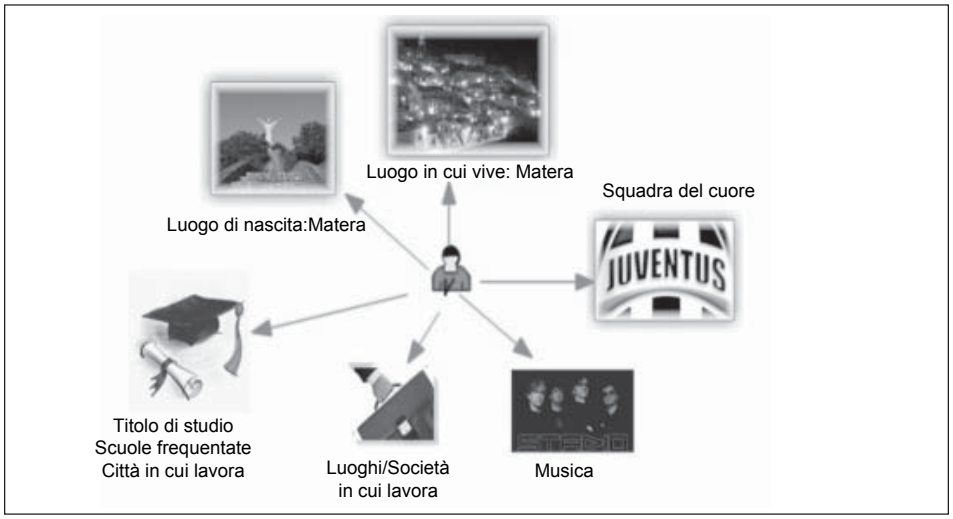


**Fig. 7: Esempio di Grafo degli interessi**

emergenza, una frase anodina o, nel caso di una mail o di un sito web, di un re-indirizzamento verso il sito web ufficiale di una società che mostra ulteriori informazioni allettanti.

Lo sviluppo dell'ingegneria sociale è in stretta relazione con lo sviluppo dei social network che diventano sia fonte di informazioni per poter studiare la vittima, ma anche il miglior mezzo per poterla contattare.

Di seguito presentiamo un esempio in cui un attaccante voglia entrare in contatto con la sua una vittima "Giuseppe Rossi" sfruttando il social network facebook (il social network più utilizzato a livello italiano e mondiale). L'attaccante inizialmente studia la vittima reperendo informazioni e realizza il grafo sociale e grafo degli interessi.

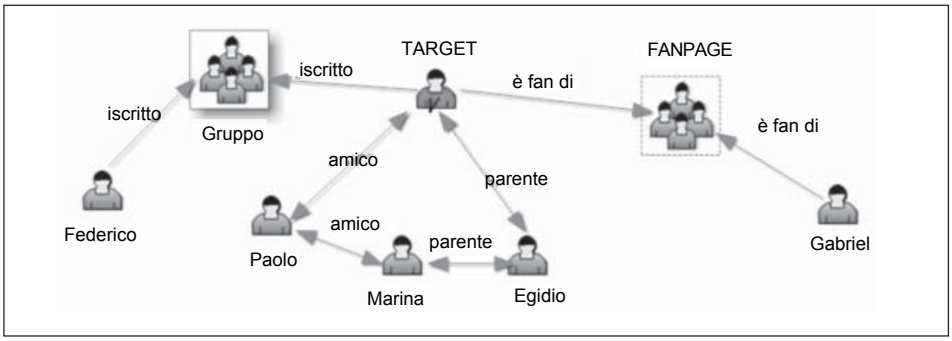


**Fig. 8: Esempio di Grafo sociale**

Realizza un profilo appetibile per ottenere l'amicizia sfruttando i concetti di identità personale (cognome, luogo di nascita,lavoro ecc.) e ottenuta l'amicizia decide la sua strategia: entrare in contatto direttamente con la vittima o ottimizzare il suo studio realizzando un grafo più accurato grazie alle informazioni ulteriori reperite e quindi creare un nuovo profilo ad hoc con cui entrare in contatto con la vittima o persone ad essa strettamente collegate.

Uno dei classici fenomeni generati dalla social engineering è quello del whaling. Il whaling è l'attacco, a mezzo informatico, che ha come obiettivo i grossi profili aziendali, per esempio l'amministratore delegato e/o i dirigenti.

IBM [5] asserisce che "si tratta, purtroppo, di una vera e propria caccia alla balena molto redditizia per i cybercriminali e un attacco con alte probabilità di successo perché costruito in maniera molto personalizzata per ogni singolo obiettivo professionale di alto profilo: infatti vengono usate le informazioni rese pubbliche dai dipendenti stessi.".

Controllare le proprie informazioni online e quelle condivise dagli utenti in stretta relazione è quindi sempre più necessario. E' bene sottolineare che lo spoofing di un profilo facebook di una persona reale costituisce reato di sostituzione di persona ed è punito con la reclusione fino ad un anno ed è procedibile d'ufficio. Inoltre l'eventuale danno d'immagine scaturito è procedibile civilmente.

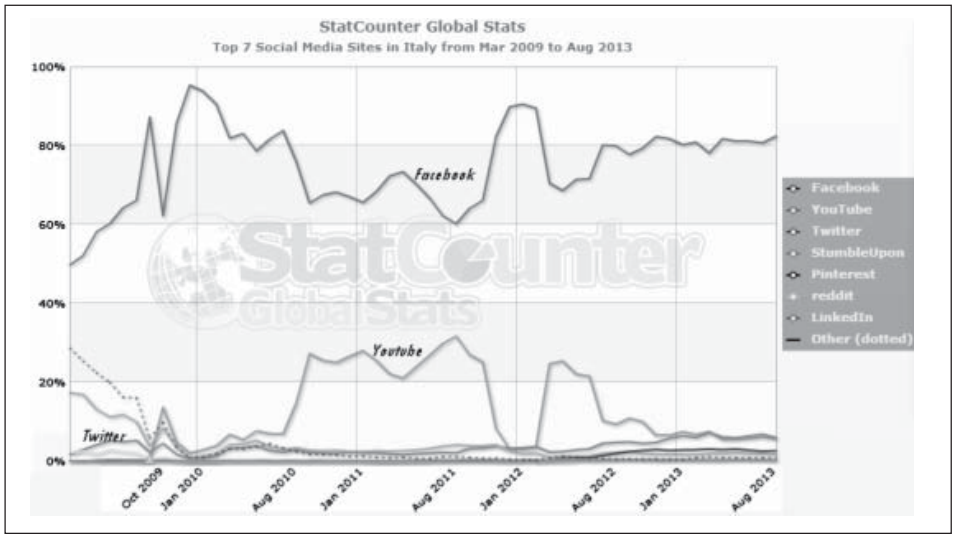


**Fig. 9: Diffusione dei social network in Italia dal 2009 a oggi [fonte: GlobalStats]**

GIUSEPPE ROSSI
Città natale: Maratea (PZ)
Città in cui vive: Matera
lavoro: Commesso in supermercato di Matera
Profili seguiti: "LAMIAJUVENTUS"
Ha frequentato istituto professionale a Potenza

1) Ricerco informazioni sulla vittima in rete (profili social netwrk, post in forum, articoli,ecc.)
2) Creo una mappa degli interessi della vittima (luogo di nascita, luogo in cui vive, luoghi frequentati, hobby, amicizie, lavoro)
3) Creo un profilo facebook appetibile per ottenere l'amicizia (con foto, dettagli, post e amici fra cui alcuni suoi amici in comune)
4) Decido il ruolo da interpretare e mosse da effettuare (messaggi privato / mail con allegato allettante che nasconde trojan, conversazione cordiale tramite messaggistica privata, nuovo profilo con nuovo target da associargli)

Possibili pagine fake allettanti:
1) Tutti i"Rossi"nel mondo [COGNOME/IDENTITÀ PERSONALE]
2) Juventus storia di un grande amore [HOBBY]
3) Steve Rossi (from Australia) [COGNOME/IDENTITÀ PERSONALE]
4) vacanzea Maratea [IDENTITÀ DEL LUOG ODI NASCITA]
5) Giovanni Sassi [CEO della ditta SUPERMERCATI MATERA]
6) Prof. Leopoldo Buccino [DOCENTE ISTITUTO PROFESSIONALE]
7) Comitatofesta dei Santo Patrono [EVENTO LOCALE]

**Fig. 10: Esempio di strategia per un attacco di ingegneria sociale su facebook**

La realizzazione di un profilo fake (con nome di fantasia) non equivale ad una sostituzione di persona, tuttavia gli eventuali reati da esso compiuti (stalking a mezzo web, diffamazione) sono punibili e sono riconducibili all'indirizzo ip pubblico collegato al post/conversazione effettuata.

## 4. CONCLUSIONI: METODI DI DIFESA

Alla luce di quanto esposto finora, si può concludere dicendo che i malintenzionati e i pirati del web hanno a disposizione diverse tecniche di falsificazione di identità utilizzabili nelle comunicazioni telematiche con cui poter raggiungere i propri obiettivi.

Ci sono però protocolli comportamentali [8] (es. cercare di instaurare un contatto diretto o in videoconferenza con l'altra persona, utilizzare esclusivamente la PEC per le comunicazioni via e-mail, usare un "protocollo personalizzato" concordato inizialmente fra le parti basato ad esempio sulla condivisione di un codice o una sequenza di step definiti per gestire le comunicazioni) o strumenti software e hardware (es. i filtri anti-phishing, gli antivirus, i firewall, i sistemi IDS) da utilizzare per difendersi da essi,e anche il buon senso può aiutare contro lo spoofing. Infatti, ad esempio, per arginare

il phishing è semplice pensare che nessun istituto bancario ci chiederà mai di aprire un sito via e-mail e di inserire la nostra password. Inoltre prima di procedere ad azioni richiesteci via mail o per telefono è sempre bene nel dubbio (se abbiamo il dubbio che si tratta di spoofing), effettuare noi una nuova telefonata o una richiesta via PEC verso i riferimenti ufficiali a cui chiedere ulteriore conferma (come in figura).

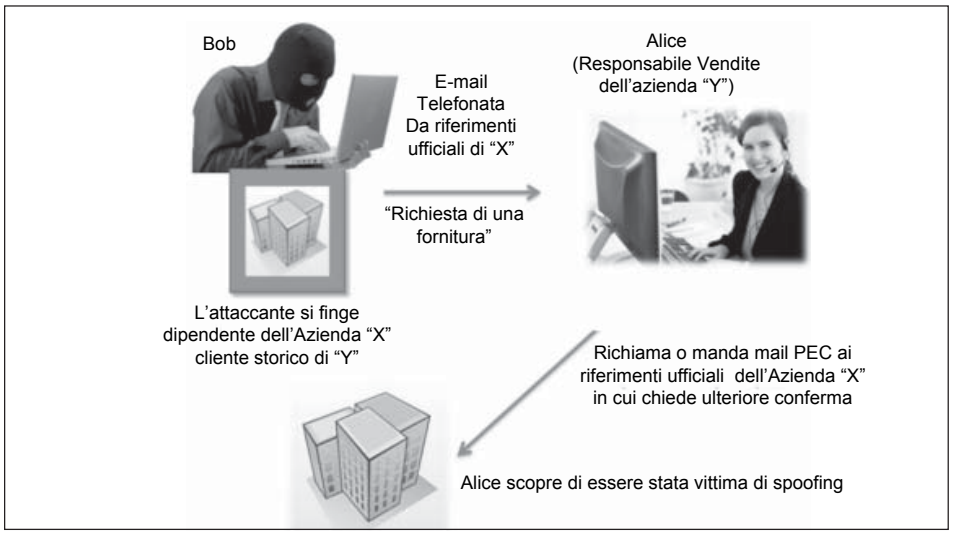


**Fig. 11: Esempio di strategia per arginare un attacco di spoofing**

Quanto ai social network, è sempre meglio tutelare la propria privacy limitando la propria cerchia di amicizie e diffidando dalla pubblicazione di proprie informazioni sensibili e di fotografie e dalla condivisione di posizioni geografiche in cui ci si trova.

Nel caso di Facebook è inoltre importante sempre segnalare se si conosce o meno un contatto che ci chiede amicizia in modo da rendere più facile a Facebook l'individuazione ed eliminazione di un profilo fake.


**Fig. 12: Esempio di controllo anti-fake effettuato da facebook**


**Fig. 13: Siemens riporta sul suo sito i seguenti dati sugli attacchi informatici (rif. anno 2010), da cui risulta che dal 2009 al 2010 sono aumentati del 50% i reati compiuti mediante VOIP, ogni 2,5 minuti avviene un attacco mediante VOIP e il 25% degli attacchi informatici sono "vishing".**

In conclusione, una realtà aziendale che sensibilizza i propri dipendenti sul pericolo dello spoofing e ne mette in atto i protocolli comportamentali e le misure precauzionali persegue un obiettivo di qualità notevole sulla sicurezza delle proprie comunicazioni telematiche, ottenendo un notevole vantaggio competitivo grazie alla riduzione del pericolo di furto di "know-how" aziendale e ottenendo la certezza delle proprie comunicazioni telematiche nel rapporto cliente-fornitore e con gli enti.

## SAFETY IN TELEMATIC: A NECESSARY GOAL TO FOLLOW

***Summary***

*The work deals with an important overview of the identity spoofing, a theme of great relevance concerning telecommunication services. Phone, fax, sms and e-mail are the main means used by social engineering for illegal actions. Goal of this article is to present this problem and related behavioral protocols or tools to use to defend themselves.*

**BIBLIOGRAFIA**

[1] **R. Russel** , "Hack Proofing", McGraw-Hill, 2003

[2] **R. Chiesa,** "Nuove e vecchie" forme di intrusione,coadiuvate da una tecnologia debole, Security Summit Roma, 2009

[3] **S.McClure**, "Hacker 7.0", McGraw-Hill, 2013

[4] **H.Schulzrinne**, "Caller ID Spoofing and Call Authentication Technology"

[5] **IBM**, "La sicurezza delle reti aziendali ai tempi di Facebook"

[6] **Microsoft**, "Visualizzazione delle intestazioni dei messaggi di posta elettronica"

[7] **R.Zunino**, **F.Carlino**, "Strutture dati di tipo sketch per l'analisi del traffico di reti informatiche", Università degli studi di Genova, 2009

[8] **K.Mitnick**, "L'arte dell'inganno", Feltrinelli, 2003

[9] **F.Cajani,G.Costabile,G.Mazzaraco**, "Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria", Giuffrè Editore, 2008

[10] **V.Santarcangelo**, "Navigare Informatici: La sicurezza ai tempi del web", Convegno c/o Hotel Palace Matera, 2011