Procura della Repubblica
presso il Tribunale di Milano

PROCEDURE INVESTIGATIVE

SUI PRIMI ACCERTAMENTI DI POLIZIA GIUDIZIARIA IN MATERIA DI REATI INFORMATICI

ESTRATTO DAL DOCUMENTO

"DIRETTIVE PER LA POLIZIA GIUDIZIARIA SUI PRIMI ACCERTAMENTI INVESTIGATIVI IN MATERIA DI REATI INFORMATICI E MODALITA' DI TRASMISSIONE DELLE RELATIVE COMUNICAZIONI DI NOTIZIA DI REATOALLA PROCURA DI MILANO"

Versione 1.0 del 5 maggio 2011

Le seguenti procedure investigative sono state formalizzate dal pool reati informatici della Procura di Milano (costituitosi nel 2004 all'interno del VII Dipartimento) in collaborazione con il Compartimento Polizia Postale e delle Comunicazioni per la Lombardia, con il supporto della Squadra Reati Informatici della Sezione Polizia Giudiziaria (che dal 2007 coadiuva il pool reati informatici).

LE TIPOLOGIE DI REATO

Di seguito viene riportata l'analisi per categorie di reati.

Occorre sottolineare che alcuni dei reati informatici qui analizzati non rientrano nelle previsioni della legge 48/2008: **in particolare NON sono reati distrettuali le seguenti ipotesi**

- **FURTO DI IDENTITÀ SEMPLICE: 494 c.p**
- **TRUFFA E-BAY: art. 640 c.p**
- **TRUFFA SU ALTRA PIATTAFORMA: art. 640 c.p.**
- **RICICLAGGIO ELETTRONICO PROVENTI ILLECITI (CYBERLAUNDERING): art. 648, 648bis c.p.**
- **CARTE CREDITO: art. 55 comma 9 d.lvo 231/2007**

  (salve le ipotesi ex art. 617-*quinquies* c.p. - installazione di apparecchiature atte ad intercettare la comunicazione intercorrente tra il *chip* della carta di credito e il sistema informatico dell'istituto di credito – o ex **art. 615-*quater* c.p.** laddove con tale condotta - di regola accompagnata anche dalla acquisizione, tramite meccanismi di videoripresa, dei relativi codici PIN all'atto della loro digitazione - abusivamente l'agente si procura codici di accesso al sistema informatico della banca)

- **DIFFAMAZIONE ONLINE: art. 595 comma 3 c.p.**

Si noti infine come le categorie CARTE CREDITO e DIFFAMAZIONI ONLINE sono state inserite in questo documento in quanto spesso inerenti a fascicoli assegnati al pool reati informatici.

DIALER (NUMERAZIONI A VALORI AGGIUNTO)

QUALIFICAZIONE GIURIDICA: art. 640-ter codice penale

FENOMENO:

A) L'utente, navigando in Internet da una rete fissa, scarica senza rendersene conto, ovvero non leggendo con attenzione le schermate di avviso sul dirottamento della chiamata verso numerazioni con un costo maggiore, taluni **programmi autoinstallanti denominati "dialer"**[1] che disconnettono il modem e lo ricollegano a numeri a valore aggiunto 899[2] e a codici satellitari ed internazionali (00), comportando dei costi molto elevati per la chiamata.

B) A tale tipologia deve essere equiparato il fenomeno delle **indebite tariffazioni per traffico dati (Internet)** in relazione a schede telefoniche cellulari, connessioni che vengono disconosciute in quanto ugualmente risultanti da bolletta telefonica.

PREGRESSE ESPERIENZE INVESTIGATIVE:

A) L'elemento essenziale per avviare l'iter conoscitivo per la dimostrazione delle frodi informatiche è la denuncia/querela, con la quale traspare che il titolare dell' utenza non riconosce di aver effettuato volontariamente il traffico sui prefissi 899 e sui codici internazionali e satellitari (00).
Sarebbe importante acquisire elementi sulle modalità di scaricamento del dialer o circa la presenza del messaggio di avviso sul costo della connessione. Tuttavia risulta complicato, per la tipologia degli elementi a disposizione della persona offesa, individuare con esattezza gli elementi di prova su cui si basa la truffa, dal momento che di regola non si riesce a dimostrare come sono stati esperiti gli artifizi e raggiri[3].

B) Quanto alle connessioni cellulari disconosciute per il traffico dati Internet, allo stato tale fenomeno è esclusivamente dovuto o a problemi tecnici ad opera del gestore (o, più spesso, ad opera dell'utente che inavvertitamente non si rendeva conto di aver attivato la connessione internet) o ad inesatta comprensione delle soglie contrattuali di tariffazione ad opera dell'utente.

[1] I dialer sono abbinati a volte a siti che propongono di scaricare contenuti, come loghi, suonerie, sfondi, file mp3, immagini e foto pornografiche, oppure sono camuffati da certificati di protezione di Internet Explorer, o sono programmi "activex", che si installano sul pc senza la necessità di scaricare alcun elemento.

[2] I codici 899 sono assegnati dal Ministero delle Comunicazioni alle società o ai gestori telefonici che ne fanno richiesta. Sono previsti una dichiarazione sostitutiva di notorietà sul tipo di servizio offerto tramite il prefisso 899 da effettuare preventivamente prima dell'avvio del servizio ed un messaggio sull'indicazione del costo della chiamata e sul tipo di servizio offerto.

[3] Si sottolinea che le società (che hanno di fatto gestito le numerazioni 899 o altre numerazioni a valore aggiunto) finora colpite da provvedimenti giudiziari si sono giustificate indicando che informavano l'utente sul dirottamento della chiamata e sul costo. Questa situazione, anche quando non è veritiera, difficilmente può essere verificata, visto che nelle querele di regola non sono riportate indicazioni su dove era collocato il dialer e sulla tipologia delle informazioni fornite all'utente.

TENTATIVO DI CONCILIAZIONE PREVENTIVO

E' opportuno che la parte lesa accerti l'esatta portata del problema chiamando il gestore telefonico[4].
Se il problema non è risolto ed si è intenzionati ad agire in giudizio per la violazione di un diritto, si deve promuovere preventivamente un tentativo di conciliazione dinanzi al Co.Re.Com. (Comitati Regionali per i Servizi Radiotelevisivi) della propria regione[5] o dinanzi agli altri organi non giurisdizionali di risoluzione delle controversie in materia di consumo[6].

Per evitare inutili perdite di tempo, si specifica che tra gli atti da fornire al Co.Re.Com non è menzionata nessuna attestazione di Uffici di Polizia (denuncia o querela), trattandosi di conciliazione fra parti di tipo extragiudiziale.

Il ricorso al giudice ordinario può, invece, avvenire solo quando il tentativo di conciliazione sia stato esperito[7] e lo stesso si sia concluso con esito negativo ovvero sia decorso il termine di 30 giorni.

a) **La promozione del tentativo di conciliazione dinanzi al Co.Re.Com.**[8], mediante formulario da inoltrarsi via fax, raccomandata o a mano, è una procedura, completamente gratuita, che va attivata prima dell'azione in giudizio in caso di controversie in materia di comunicazioni elettroniche tra utenti finali ed operatori, inerenti al mancato rispetto delle disposizioni relative al servizio universale ed ai diritti degli utenti finali stabilite dalle norme legislative, dalle delibere dell'AGCOM, dalle condizioni contrattuali e dalle carte dei servizi.

Dal momento della proposizione del tentativo obbligatorio di conciliazione i termini per agire in giudizio sono sospesi e riprendono a decorrere dalla scadenza del termine di conclusione del procedimento, che è pari a 30 giorni dalla data di proposizione dell'istanza.

Nell'istanza presentata al Co.Re.Com devono essere indicati, a pena di inammissibilità, i dati previsti dall'art.7 della delibera dell'AGCOM n.173/07/CONS, ovvero:

- nome e cognome, residenza o domicilio dell'utente;
- numero dell'utenza in caso di servizi telefonici;
- denominazione e sede dell'operatore;
- gli eventuali tentativi già esperiti per la composizione della controversia;
- le richieste dell'istante;
-i documenti che si allegano.

[4] Alcune gestori telefonici (ad esempio Telecom e H3G) hanno siglato protocolli di intesa con la maggiori Associazioni di Consumatori, che consente ai propri clienti di avvalersi, autonomamente o attraverso un'Associazione di Consumatori, di una procedura conciliativa alternativa a quelle già previste.
[5] Il Co.Re.Com della Lombardia è abilitato ad esercitare tale funzione. La sua sede è a Milano in via Lazzaroni nr.3, tel.02/67482300, fax 02/67482701-707, e-mail *corecom@consiglio.regione.lombardia.it*, sito Internet *www.corecomlombardia.it*
[6] Di seguito verranno indicati quali sono gli organi non giurisdizionali di risoluzione delle controversie in materia di consumo.
[7] Con sentenza nr. 24334/08 del 28.5.2008 la Sezione Terza Civile della Suprema Corte di cassazione ha indicato che "*l'attore, prima di agire in giudizio, è tenuto a promuovere preventivamente un tentativo di conciliazione dinanzi al Corecom competente per territorio*".
[8] La procedura è disciplinata dalla delibera dell'AGCM n.173/07/CONS, presente sul sito *www.agcom.it.*

b) Gli **altri organi non giurisdizionali di risoluzione delle controversie in materia di consumo** sono quelli previsti dall'art.141 commi 2 e 3 del Codice di Consumo[9] e gli organismi istituiti con accordi tra gli operatori ed associazioni di consumatori rappresentative a livello nazionale, purchè detti organismi operino a livello gratuito e rispettino i principi di trasparenza, equità e efficacia di cui alla raccomandazione 2001/310/CE. L'elenco aggiornato degli organi di conciliazione prima richiamati è disponibile sul sito web dell'Autorità *www.agcom.it*[10].

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

Come già ricordato, la persona offesa – in caso voglia presentare una vera e propria querela e quindi fare avvio alle indagini - dovrà fornire alle Forze dell'Ordine le **seguenti informazioni**:

- copia della bolletta telefonica ove saranno indicate le chiamate disconosciute;
- indicazioni su come è stato scaricato il *dialer* e su come si adopera e si è protetto il computer;
- tipologia del contratto utilizzato per il traffico dati Internet da telefono cellulare.

[9] Si riporta di seguito l'art.141 del Codice di Consumo, previsto dal d.lvo. 206/05, sulla "composizione extragiudiziale delle controversie".
"*1. Nei rapporti tra consumatore e professionista, le parti possono avviare procedure di composizione extragiudiziale per la risoluzione delle controversie in materia di consumo, anche in via telematica.*
2. Il Ministero delle attività produttive, d'intesa con il Ministero della giustizia, comunica alla Commissione europea l'elenco degli organi di composizione extragiudiziale delle controversie in materia di consumo che si conformano ai principi della raccomandazione 98/257/CE della Commissione, del 30 marzo 1998, riguardante i principi applicabili agli organi responsabili per la risoluzione extragiudiziale delle controversie in materia di consumo e della raccomandazione 2001/310/CE della Commissione, del 4 aprile 2001, concernente i principi applicabili agli organi extragiudiziali che partecipano alla risoluzione extragiudiziale delle controversie in materia di consumo. Il Ministero delle attività produttive, d'intesa con il Ministero della giustizia, assicura, altresì, gli ulteriori adempimenti connessi all'attuazione della risoluzione del Consiglio dell'Unione europea del 25 maggio 2000, 2000/C 155/01, relativa ad una rete comunitaria di organi nazionali per la risoluzione extragiudiziale delle controversie in materia di consumo.
3. In ogni caso, si considerano organi di composizione extragiudiziale delle controversie ai sensi del comma 2 quelli costituiti ai sensi dell'articolo 4 della legge 29 dicembre 1993, n. 580, dalle camere di commercio, industria, artigianato e agricoltura.
4. Non sono vessatorie le clausole inserite nei contratti dei consumatori aventi ad oggetto il ricorso ad organi che si conformano alle disposizioni di cui al presente articolo.
5. Il consumatore non può essere privato in nessun caso del diritto di adire il giudice competente qualunque sia l'esito della procedura di composizione extragiudiziale".

[10] Per esempio sono organi di composizione extragiudiziale delle controversie il Giudice di Pace e la Camera di Commercio.

□ FURTO DI IDENTITÀ SEMPLICE

QUALIFICAZIONE GIURIDICA: artt. 494 codice penale [11]

FENOMENO: trattasi di un fenomeno variegato, ricomprendente:

A) tutti i tentativi di *phishing*[12] tramite invio di *e-mail* (in questo caso la più corretta qualificazione giuridica deve essere quella di 56, 494, 640-ter c.p.)

B) altri furti di identità, anche consumati, rispetto ai quali la persona offesa non lamenta di aver ricevuto – al momento della denuncia/querela – un danno.

PREGRESSE ESPERIENZE INVESTIGATIVE:

A) Gli accertamenti di tipo tecnico informatico sugli illeciti riconducibili al fenomeno del "*phishing*" risultano spesso impossibili alla luce delle informazioni raccolte in sede di denuncia/querela poiché i link relativi ai siti clone sono visualizzabili a partire dall'*e-mail* in formato elettronico e per breve tempo.
Se tali dati vengono acquisiti, le verifiche, anche se teoricamente perfezionabili, non forniscono elementi utili per l'identificazione dell' autore dei reati posti in essere, dato che si è visto in pregresse indagini che l'invio dei messaggi avviene dall'estero, che l'ubicazione delle macchine ospitanti siti web clone è estera e che vengono usate macchine già violate o senza protezioni; tali circostanze non permettono di svolgere ulteriori attività investigative senza il ricorso di una rogatoria internazionale (spesso impossibile perché non sussistono le condizioni giuridiche di reciprocità con

[11] Cass, *Sez*. 5, Sentenza n. 46674 *del* 08/11/2007 Ud. (dep. 14/12/2007) in CED 238504: "*Integra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un "account" di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete 'internet' nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale)*"

[12] Il termine "*phishing*" indica un'attività fraudolenta in genere perfezionata sulla rete Internet, che consiste nella predisposizione di tecniche idonee a carpire fraudolentemente dati personali sensibili (quelli più di interesse sono le numerazione di carte di credito, i conti correnti *online*, i codici relativi a depositi effettuati in banca ed i pin dei bancomat, ovvero informazioni che per essere ottenute richiedono anche l'involontaria ma incauta collaborazione della vittima).
L'autore dell'attacco di *phishing* si limita ad inviare ad un numero elevato di utenti della Rete un elemento di stimolo, che in genere consiste in un messaggio di posta elettronica o di un virus informatico, sperando nel ritorno di dati sensibili (*user-id* e *password*) da parte delle vittime, così da accedere a loro conto corrente bancario o postale.
Con l'invio del messaggio di posta elettronica, l'intenzione dei truffatori è quella di far visualizzare il sito relativo al link inserito nell'*e-mail*, ovvero una pagina web clone dell'istituto di credito gestita dai criminali, ove l'utente viene invogliato ad inserire le proprie credenziali di accesso, così acquisite per gli usi illeciti.
Cliccando sul link proposto, infatti, **la pagina che viene caricata non è quella della banca,** dell'istituto o della società corretta, **ma quella di un sito web creato ad arte per consentire all'utente malintenzionato di sottrarre e memorizzare le informazioni fornite da utenti ignari**: informazioni riservate e confidenziali come il nome utente e la password.
Più difficile da percepire risulta l'attacco informatico allorché lo stesso si realizzi attraverso l'invio di un virus - a volte contenuto all'interno della posta elettronica, a volte trasmesso attraverso prassi di navigazione o di sollecitazione di altri servizi Internet se il PC non è dotato di idonea protezione -, che una volta subdolamente installatosi nel personal computer della vittima ne possa carpire i dati sensibili per trasmetterli riservatamente in un secondo momento al truffatore.
Una volta che i criminali abbiano avuto accesso, con le modalità prima descritte, ai dati delle vittime, sono pronti per la sottrazione illecita del denaro contenuto nei loro conti e di far perdere le loro tracce mediante trasferimenti bancari, avvalendosi della complicità di più o meno consapevoli intermediari.

lo stato estero da cui proviene l'attacco), il cui esito, anche se potenzialmente positivo, comunque difficilmente consentirebbe di giungere all'individuazione dei responsabili della frode.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

Oltre a quanto già indicato[13], occorrerà innanzitutto verificare – dandone ampia descrizione nel testo della querela – **cosa è stato fatto in concreto con i propri dati**.

E' importante ribadire che se la persona offesa ha cancellato la *e-mail* di *phishing* ricevuta, nessun tipo di accertamento sarà possibile.

[13] Ossia: nome del servizio attivato in frode e/o a nome del denunciante; indicazioni utili circa il profilo attivato illegittimamente; documentazione relativa all'attività illecita compiuta.

□ VIOLAZIONE ACCOUNT

QUALIFICAZIONE GIURIDICA: artt. 494, 615-ter codice penale

FENOMENO:

Trattasi di un fenomeno più complesso rispetto al precedente, ricomprendente in particolare:

A) **violazione account eBay o di altre piattaforme di commercio elettronico (o di bacheche annunci vendita)**, al fine di porre fittiziamente in vendita su Internet – avvalendosi di una identità non corrispondente al reale venditore - beni con l'intento di non inviarli all'acquirente, così ottenendo l'ingiusto profitto del prezzo che di regola viene corrisposto tramite pagamenti elettronici prima dell'invio del bene. Di tale fenomeno spesso l'utente (che ha subito la violazione del proprio account) ne viene a conoscenza a seguito della comunicazione che lo stesso si vede recapitare dall'Istituto di recupero crediti Intrum Justitia[14] o altri istituti di recupero crediti di transazioni *online*[15]

B) **violazione/acquisizione indebita dell' account personale/profilo Facebook o di quello relativo ad altre piattaforme di social network**

PREGRESSE ESPERIENZE INVESTIGATIVE:

L' acquisizione fraudolenta dell'*account* spesso avviene con tecniche di *social enginering*, tramite invio di *e-mail* che inducono il legittimo titolare a rivelare a terzi (che, solo apparentemente, sono ricollegabili ai gestori della piattaforma elettronica) i dati relativi al proprio *account*

L'esperienza investigativa acquisita in analoghi casi dal pool reati informatici di questa Procura e dalla Polizia Postale di Milano ha consentito di determinare come tali azioni di regola provengono da persone che, anche avvalendosi di strumenti informatici, operano in territorio estero e pertanto anche eventuali richieste di assistenza giudiziaria, a mezzo di rogatorie, porterebbero ad esiti negativi considerato peraltro i limitati termini di conservazione dei dati informatici a cura dei gestori di telecomunicazione.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

E' bene ricordare come, prima di rivolgersi alle Forze dell'Ordine, sia possibile sollecitare (autonomamente e tempestivamente) il blocco di tale *account* ad opera del gestore della piattaforma, non avendo la stessa ancora subito un pregiudizio di carattere economico/morale da tale azione indebita ad opera di terzi.

[14] Quanto a eBay.

[15] Tali istituti infatti sono a richiedere all'utente (che, solo fittiziamente, risulta aver operato una vendita online ma in realtà si è visto artatamente rubato il proprio account) il costo della intermediazione, come da contratto che regola il commercio elettronico a mezzo della piattaforma.

Come nel caso di furto di identità semplice (cfr. retro) occorrerà indicare alla Polizia Giudiziaria innanzitutto se tale ipotesi ha causato un effettivo danno alla persona offesa.

In caso di comunicazioni ad opera di istituti di recupero credito, la persona offesa dovrà allegarne copia.

La persona offesa dovrà allegare anche tutte le informazioni utili attestanti l'avvenuta violazione dell'account. In particolare occorrerà indicare

- se si tratti di violazione di un account/profili già esistente,
- se invece è stato creato ex novo un account/ profilo: in questo caso la parte lesa dovrà indicare gli aspetti specifici di riconducibilità di tale account/profilo alla sua persona (per escludere, per esempio, che si tratti di mera omonimia).

□ ACCESSO EMAIL

QUALIFICAZIONE GIURIDICA: art. 615-ter codice penale

FENOMENO:

A) trattasi di una ipotesi specifica rispetto a quella precedente che, per la sua diffusività, merita di essere trattata separatamente. Non sempre poi la persona offesa ha prova dell'utilizzo indebito di tale casella di posta elettronica e, con esso, del realizzarsi del furto di identità ex art. 494 c.p.

B) a tale ipotesi devono essere equiparati tutti i denunciati **accessi illegittimi ad altri account di comunicazione**, quali ad esempio chat (ipotesi frequente il sistema messanger di Microsoft denominato MSM).

PREGRESSE ESPERIENZE INVESTIGATIVE:

Spesso il fenomeno è ricollegabile ad un mero malfunzionamento della casella di posta elettronica e, dalla lettura degli atti presentati alle Forze dell'Ordine, non emerge alcun ulteriore elemento tale da suffragare ipotesi alternative aventi rilievo penale.

Si è peraltro rilevato che molto spesso l'atto è presentato unicamente per disconoscere eventuali attività effettuate con la casella a titolo precauzionale o per dichiararsi estranei alla divulgazione di contenuti relativi a messaggi inviati, senza l'effettiva intenzione di individuare i responsabile degli abusi: in tal caso è sufficiente presentare una **mera denuncia.**
Peraltro spesso il fenomeno riguarda episodi legati al cattivo funzionamento della posta elettronica o aspetti marginali e prettamente privati, senza la commissione di particolari danni economici.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

Per far emergere l'eventuale rilevanza penale dei fatti ed ove si ritenga di voler proporre una querela, risulta pertanto indispensabile circostanziarla dei seguenti aspetti:

- utilizzo usuale della casella di posta elettronica (lavoro, tempo libero, altro utilizzo);
- password di accesso all' *e-mail*[16] o comunque il suo grado di robustezza (quanti caratteri, se anche alfanumerici); domanda segreta eventualmente pre-impostata per ottenere dal sistema la password in caso di dimenticanza; informazioni sulle persone che conoscevano tale password o che avrebbero potuto conoscerla (per prossimità/frequentazione con l'utente);
- luogo di consultazione della casella di posta elettronica; tipo di collegamento usato;
- sistema operativo del PC usato abitualmente per collegarsi alla posta elettronica e descrizione dell' eventuali aggiornamenti di sicurezza configurate; misure di protezione adottate a tutela

[16] Si specifica che è fondamentale riportare nella querela la password di accesso alla casella, poiché il Pubblico Ministero dovrà indicare che l'indagato ha adoperato la specifica password di accesso del querelante per far uso del servizio mail e quindi prendere cognizione del contenuto, nel momento in cui formulerà il rinvio a giudizio del responsabile dell'abuso.

della password di accesso all'e-mail; misure di protezione adottate a tutela del PC di casa o del posto di lavoro, usato abitualmente per leggere tale casella di posta elettronica; se l'utente possiede i privilegi di amministrazione di tale computer;
- modalità di percezione dell'utilizzo indebito della casella/periodo temporale nel quale la casella è stata violata;
- contenuto della casella al momento dei fatti, con particolare riferimento alla presenza di messaggi di grande rilevanza;

Se si tratta di **casella di posta elettronica aziendale**, è opportuno premunirsi di una relazione tecnica dell'amministratore di sistema dell'azienda.

Occorre infine evidenziare nella querela se la casella di posta elettronica è abbinata ad altri servizi o conti correnti online (indicando le risposte positive nella querela): a tal fine, indipendentemente dalla presentazione della querela, bisognerà provvedere al più presto al cambio del riferimento e-mail per tali servizi.

□ ALTRO ACCESSO ABUSIVO

QUALIFICAZIONE GIURIDICA: 615-ter c.p.

FENOMENO:

1) trattasi delle vere e proprie intrusioni informatiche, spesso denunciate da società o gestori di siti web/sistemi di comunicazione

2) sempre più spesso si registrano episodi **di violazioni di centralini telefonici VOIP[17],** spesso denunciate da società, di frequente compiute nei fine settimana, che permettono l'effettuazione in frode di traffico telefonico diretto a telefoni cellulari con profilo di autoricarica, numerazioni estere e satellitari o a codici a valore aggiunto (**e quindi trattasi anche di ipotesi ex art. 640-ter c.p.p.**)

A volte la causa dell'uso fraudolento del sistema telefonico è da rilevarsi in una falla aperta nell'infrastruttura (vulnerabilità dei firewall aziendali, bug o errate configurazioni dei sistema VoIP, previsione di password di accesso non robuste o impostate di default dal costruttore), che è sfruttata per l'instradamento del traffico telefonico.

Talvolta l'operatore telefonico al quale si appoggia la società per inoltrare le proprie telefonate, si accorge del traffico anomalo generato e blocca le chiamate con destinazioni internazionali.

PREGRESSE ESPERIENZE INVESTIGATIVE:

Gli eventi informatici che vengono indicati in sede di querela necessitano di un **riscontro tecnico-informatico** che la stessa persona offesa nella maggior parte dei casi può e deve allegare, producendo essa stessa tutte le evidenze informatiche (ad iniziare dai *file* di *log* e, nel caso sub 2) anche della fattura del traffico disconosciuto) registrate nei relativi sistemi informatici/di telecomunicazione interessati e fornendo indicazioni utili per il proseguo delle indagini.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

Appare evidente che la stessa persona offesa possa acquisire – anche a mezzo di consulente tecnico di parte – e trasmettere alla Polizia Giudiziaria, anche **ad integrazione della originaria denuncia querela**, tali informazioni anche in formato elettronico (su supporti non riscrivibili e firmati dalla persona che materialmente ha proceduto alla masterizzazione) quali:

- informazioni sulla configurazione del centralino telefonico e sull'accesso abusivo subito[18], fornendo i file di log anche in formato

[17] Con telecomunicazioni in **Voice over IP** (*Voce tramite protocollo Internet*), acronimo **VoIP**, si intende una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o un'altra rete dedicata che utilizza il protocollo IP senza connessione per il trasporto dati (tratto da Wikipedia).

[18] In particolare: *file* di *log* relativi agli accessi disconosciuti; tipo e versione del sistema in uso; protocolli di comunicazione utilizzati; descrizione del tipo di operazioni illecite e dei danni accertati con eventuale loro qualificazione; nominativi delle persone informate sui fatti; *backup* dei file interessati dalle modifiche o contenenti informazioni relative all'attacco.

elettronico (sempre su supporti non riscrivibili e firmati dalla persona che materialmente ha proceduto alla masterizzazione).

La stessa persona offesa dovrà indicare con precisione i nominativi dei testi da sentire, con le circostanze sulle quali le stesse potranno utilmente riferire, e produrre fin da subito eventuali rapporti interni aziendali circa la ricostruzione dell'incidente informatico.

Come già indicato, nel caso sub 2) il querelante dovrà inoltre fornire la fattura telefonica possibilmente con dettaglio del traffico anche parzialmente oscurato (così emergerà subito la destinazione del traffico-estero o verso numerazioni a valore aggiunto).

□ **E-BAY TRUFFA**
□ **TRUFFA SU ALTRA PIATTAFORMA**

QUALIFICAZIONE GIURIDICA: art. 640 c.p.

FENOMENO:

A) Gli utenti si accordano, tramite servizi di commercio *online* (in particolare eBay[19]), per vendere ed acquistare della merce, prevedendo come modalità di pagamento

- il trasferimento di denaro tramite Western Union/Money Gram,
- l'uso di vaglia *online*,
- l'effettuazione di ricariche di carte di credito prepagate (ad esempio Postepay)
- altri sistemi di pagamento elettronico (es. paypal)

B) Molto diffuso anche l'utilizzo di assegni circolari falsi (molto spesso stranieri): tale tipologia di truffa è inizialmente emersa soprattutto in relazione alla piattaforma di *secondamano.it*, le cui modalità sono peraltro segnalate agli utenti dal relativo sito:

> ***Offerta di pagamento superiore al prezzo del bene venduto***
> *La truffa comincia con la ricezione di una mail, da parte di un ipotetico acquirente, interessato al prodotto che vorresti vendere. Si tratta generalmente di un acquirente che vive all'estero e che ti pagherà con un assegno. Generalmente il presunto acquirente ha molta fretta di acquistare l'oggetto e dice di avere un contatto in Italia che verrà a prendere il prodotto dove preferisci. In certi casi potrebbe offrirti due o tre volte la cifra da te richiesta a garanzia, e che potrai restituirgli la differenza alla ricezione del bene. Altre volte, potrebbe tentare di convincerti che l'assegno che ti invierà ha un importo maggiore perché parte di esso serve a sbrigare pratiche doganali o cose del genere. Quello che invece è certo è che se il bene, ad esempio, costa 2.000 euro e il presunto acquirente ti invia un assegno da 6.000 euro, ti chiederà senz'altro di inviargli la differenza. Attenzione perché la banca può accettare l'assegno e impiegare settimane prima di comunicarti che invece non è regolare e che tu hai inviato denaro a un'organizzazione criminale. Altre truffe simili nascono dall'utilizzo di ricevute di bonifico online falsificate o in caso di venditori che raccomandano un servizio di deposito a garanzia sconosciuto.*

PREGRESSE ESPERIENZE INVESTIGATIVE:

Dall'esperienza investigativa maturata si è rilevato che le connessioni ad Internet usate per commettere gli illeciti vengono effettuate a partire da macchine in precedenza violate (cd. macchine “bucate” o “zombie”[20]) o da postazioni presenti all'estero.
Tuttavia, può portare a risultati più efficaci – al fine di identificare l’autore dei reati – evidenziare gli strumenti di pagamento adoperati.

[19] Si noti come tale piattaforma di commercio elettronico, allo stato, accetti solo come modalità di pagamento quelle legate a ricariche postepay o tramite paypal.
[20] Così vengono anche chiamati i computer che sono controllati dall'attaccante.

Quanto al fenomeno sub B), trattandosi di condotte criminose commesse di regola dall'estero, i relativi accertamenti investigativi saranno di difficile esecuzione se non con ricorso a collaborazioni di Polizia Giudiziaria di differenti Stati e/o richieste rogatoriali

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

La persona offesa dovrà fornire tutti gli elementi utili al proseguo delle indagini (indicando innanzitutto la piattaforma di commercio elettronico/sito internet relativo all'acquisito), ed in particolare allegare

- tutti i dati relativi alla inserzione/annuncio di vendita apparso sulle pagine Internet, comprensivo di URL[21] completa della pagina relativa alla vendita; dovrà altresì indicare eventuali dati relativi alla partita IVA/codice fiscale del venditore (ove reperibili dalla inserzione/annuncio o dal sito internet);
- copia (meglio se informatica) di tutte le comunicazioni intercorse via e-mail (comprensive degli *header*) con il sedicente venditore, indicando altresì – in caso di contatti telefonici – il numero chiamato ed (ove disponibile) anche il numero chiamante;
- indicazione degli elementi che fanno presuppone la truffa, e segnatamente gli artifizi e raggiri posti in essere dal sedicente venditore per conseguire l'ingiusto profitto, che sostanziano il reato distinguendolo dal semplice inadempimento di natura civilistica;

[21] Un **Uniform Resource Locator** o **URL** è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, come un documento o un'immagine (es. www.giustizia.it).

□ BONIFICO/RICARICA DISCONOSCIUTA (PHISHING)

QUALIFICAZIONE GIURIDICA: art. 110, 640, 648 c.p.

FENOMENO:

In tali casi la persona offesa si lamenta della fraudolenta captazione - tramite la già indicata tecnica del *phishing* - di informazioni e dati riservati relativi a

- carte di credito
- carte ricaricabili (es. postepay)
- conti correnti *online*

con relativo utilizzo illecito, ad opera di terzi, tramite operazioni *online* idonee a privarlo di ingenti somme di denaro.

PREGRESSE ESPERIENZE INVESTIGATIVE:

Abbiamo già accennato come gli accertamenti di tipo tecnico informatico sugli illeciti riconducibili al fenomeno del "*phishing*" risultano spesso impossibili alla luce delle informazioni raccolte in sede di denuncia/querela.
Vi sono invece altri approfondimenti esperibili, finalizzati a reperire riscontri oggettivi utili per l'individuazione del beneficiario finale del trasferimento dei fondi.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

La persona offesa dovrà fornire tutti gli elementi utili al prosieguo delle indagini, ed in particolare allegare

- l'estratto conto completo, dal quale risultino i dati precisi della **destinazione finale** delle somme di denaro.

Dovrà altresì dare indicazione

- se prima delle spendite fraudolente è stato ricevuto un messaggio di posta elettronica relativo al *phishing*; in caso positivo, *header* (intestazione) dell'e-*mail* di *phishing* e messaggio in formato elettronico;
- di come sono custodite le credenziali di accesso (password, *token*[22]) e del fatto che la persona offesa abbia recentemente subito attività anomale (quali un furto).

Dovrà contestualmente essere ben evidenziato se le movimentazioni disconosciute sono state fatte per effettuare

[22] Un **token per la sicurezza** (chiamato anche **token hardware**, **token per l'autenticazione**, **token crittografico**, o semplicemente **token**) è un dispositivo fisico necessario per effettuare un'autenticazione (tipicamente una autenticazione a due fattori). Un *token* si presenta spesso sotto forma di dispositivo elettronico portatile di piccole dimensioni, alimentato a batteria con autonomia nell'ordine di qualche anno, dotato di uno schermo e talvolta di una tastiera numerica. Alcuni *token* possono essere collegati ad un computer tramite una porta USB per facilitare lo scambio di dati. Un *token* può anche essere di tipo software, ove le informazioni necessarie risiedono direttamente nel computer dell'utente, e non in un oggetto esterno (tratto da wikipedia).

- bonifici bancari su altri conti correnti[23],
- ricariche di Carte prepagate[24]
- ricariche di sim card di telefonia mobile[25],
- pagamenti di utenze tramite il sito "poste.it"[26] o altri siti web che consentano pagamenti *online*

[23] Nei casi di bonifico bancario su altri conti correnti deve essere avanzata richiesta di fornire i dati dell'intestatario del conto beneficario. Per tale modalità di illecito è infatti necessario l'intervento di un soggetto consenziente che sia intestatario di un conto corrente di appoggio, che procede in genere al prelievo del denaro movimentato sul suo conto ed all'invio dello stesso all'estero per mezzo di società di intermediazione finanziaria quali Western Union o Moneygram, trattenendo una percentuale prestabilita per l'illecita prestazione.

[24] Si tratta di carte prepagate emesse da istituti di credito o da Poste Italiane e sono spesso attivate con documenti falsi. Il loro possessore, una volta avuta contezza dell'accredito del denaro, procede al prelievo delle somme con una operazione presso sportelli ATM, che non lascia traccia documentale e che difficilmente consente l'identificazione a mezzo videoripresa, atteso che le registrazioni stesse, laddove funzionanti, vengono conservate per tempi assai ridotti.

[25] Si tratterà anche qui di avanzare ai rispettivi gestori telefonici richiesta di fornire i dati dell'intestatario della scheda sim. **Tuttavia tali accertamenti, di regola, hanno esiti negativi in quanto si tratta di sim intestate fittiziamente od in relazione alle quali non è possibile identificare con certezza l'utilizzatore.**

[26] Il denaro sottratto viene utilizzato per effettuare ricariche di telefoni cellulari o per il pagamento di utenze di soggetti realmente esistenti attraverso il sito poste.it.

□ RICICLAGGIO ELETTRONICO PROVENTI ILLECITI (CYBERLAUNDERING)

QUALIFICAZIONE GIURIDICA: art. 648, 648-bis c.p.

FENOMENO:

Gli esiti delle indagini condotte fin dal 2005 dalla Procura di Milano in relazione al fenomeno del cd. *phishing* che ha interessato numerosi istituti di credito italiani hanno evidenziato

- una serie di soggetti italiani che, previa precedente comunicazione delle loro coordinate bancarie a soggetti di regola tutti operanti dall'estero, si rendevano disponibili a prelevare in contanti somme di denaro fatte confluire sui loro conti a seguito di *bonifici online;*

- una serie di soggetti, spesso residenti in paesi dell'Est Europa, che risultavano beneficiari di somme di denaro fatte loro pervenire, tramite trasferimenti WESTERN UNION e/o MONEY GRAM da parte degli stessi soggetti italiani di cui sopra;

Tali *bonifici online* sono stati effettuati, in danno degli ignari titolari dei rispettivi conti ordinanti, previa illecita acquisizione delle rispettive credenziali (*username* e *password*, necessarie per le relative operazioni di *home banking*);

I titolari dei conti correnti italiani (cd. *financial manager*[27]) beneficiari di tali bonifici *online*, ritenendo di ottemperare ad un contratto di lavoro[28], trattengono una percentuale di quanto a loro indebitamente accreditato e trasferiscono la residua somma a persone prevalentemente residenti nei paesi dell'Est Europa con le modalità sopra indicate.

PREGRESSE ESPERIENZE INVESTIGATIVE:

Quanto agli accertamenti idonei ad identificare le persone operanti all'estero, dall'esperienza investigativa maturata si è rilevato che le connessioni ad Internet usate per attuare il richiamato *modus operandi* vengono effettuate a partire da macchine in precedenza violate o da postazioni situate all'estero.

Quanto alla condotta posta in essere dai beneficiari dei bonifici *online*, essa deve essere oggettivamente qualificata ai sensi dell'art. **648-bis c.p.**, essendo idonea a porre in essere una attività di riciclaggio di somme di denaro provento di reato (frode informatica, allo stato delle indagini commessa da soggetti tutti operanti all'estero). Ovvero ai sensi dell'art. **648 c.p.** laddove, come verificatosi in alcuni casi, non sia avvenuto il successivo ritrasferimento dopo l'incasso.

[27] L'intermediazione dei *financial manager* (operatore finanziario) si rende necessaria perché il sistema di home banking italiano non consente bonifici verso l'estero se non a seguito di specifici controlli ulteriori che farebbero venire allo scoperto la truffa

[28] Si noti come il Tribunale di Milano ed altri Giudici in Italia hanno tuttavia già emesso importanti sentenze di condanna nei confronti di tali soggetti, ritenendo sussistente la consapevolezza della provenienza illecita delle somme.

□ CARTE CREDITO

QUALFICAZIONE GIURIDICA: art. 55 comma 9 D.lvo 21 novembre 2007, n. 231[29]

FENOMENO:

1) nella maggior parte dei casi la persona offesa disconosce alcuni pagamenti, effettati a sua insaputa.

2) capita spesso che la Polizia Giudiziaria intervenga nei pressi di istituti di credito o di sportelli bancomat. Solamente laddove gli indagati siano trovati nel materiale possesso di carte di credito sarà possibile invocare l'art. 55 comma 9 d.lvo 231/2007 al fine dell'arresto nella flagranza del reato[30].

PREGRESSE ESPERIENZE INVESTIGATIVE:

Gli accertamenti sulle spendite effettuate in Italia presso esercizi commerciali a distanza di tempo rispetto ai fatti non permettono l'ottenimento di indicazioni utili, a causa delle scarse indicazioni che l'addetto al pagamento può fornire, tranne nei casi di spese rilevanti in negozi con limitato flusso di clienti (per esempio gioiellerie o concessionari di grandi marche).
Può essere importante risalire con immediatezza al punto di compromissione (ovvero l'ultimo luogo ove è stata spesa la carta in maniera genuina) per capire se le carte vengono acquisite con sistemi fraudolenti da personale interno: tuttavia di regola l'analisi delle spendite fraudolente finalizzata alla ricerca di punti di compromissione viene effettuata direttamente dai gestori delle carte di credito, che predispongono autonomamente specifiche e complessive denunce/querele alla luce di quanto emerso da tali analisi.
In caso di prelievi presso sportelli bancomat dotati di telecamere, infine, solo raramente è possibile rinvenire indicazioni valide a causa del breve periodo di conservazione delle immagini nel sistema di telesorveglianza (di solito non oltre le 24/48 ore), laddove funzionante e opportunamente posizionato.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

L' estratto conto della carta di credito o della lista dei movimenti disconosciuti effettuati con bancomat è allegato indispensabile alla denuncia.

Come poi già ricordato, occorre richiedere in sede di denuncia/querela:

[29] Ove dalla lettura degli atti emerga come accertato **unicamente** l'avvenuto utilizzo indebito di una carta, il fascicolo deve essere iscritto solo per tale reato e non anche per l'art. 640-ter c.p.: sul punto anche provvedimento Procura Generale della Repubblica presso Corte di Appello di Milano, 1/10 Reg. contrasti, del 18.1.2010, che ha ritenuto "*interessanti ipotesi… e non idonee a determinare la competenza*" le considerazioni circa un precedente accesso abusivo al sistema informatico del correntista/possessore della carta di credito o di una frode informatica ex art. 640-ter c.p. ai suoi danni.
[30] Lo stesso varrà, anche se tuttavia è ipotesi di difficile verificazione, ove siano ritrovate persone nell'atto di falsificare carte di credito o nell'atto di cedere/acquisire carte contraffatte.

- indicazione del numero della carta di debito/credito;
- nome della società proprietaria e della banca emittente possibilmente con l'indicazione della filiale e del relativo numero di conto corrente;
- copia degli estratti conti dei movimenti degli ultimi mesi, se possibile;
- copia fotostatica fronte-retro della carta di credito/debito, se ancora in possesso del denunciante e se ritenuto necessario.

□ DIFFAMAZIONE ONLINE

QUALFICAZIONE GIURIDICA: art. 595 comma 3 c.p.

FENOMENO: la persona offesa lamenta una pubblicazione sulla rete internet (sito Internet, blog, forum online) lesiva del proprio onore/reputazione.

Quanto agli altri fenomeni più marginali (e-mail o SMS diffamatori), gli stessi non rientrano tra i fascicoli assegnati al pool reati informatici e quindi non verranno trattati nel proseguo.

PREGRESSE ESPERIENZE INVESTIGATIVE:

Registriamo un aumento esponenziale di fascicoli che riguardano siti Internet o blog all'estero. In siffatti casi, di regola, gli accertamenti utili a risalire all'autore del reato non sono possibili.

INFORMAZIONI DA FORNIRE IN SEDE DI QUERELA:

Occorrerà acquisire dalla persona offesa la copia della pagina web (o del messaggio sul forum o del blog) offensiva. In mancanza, la persona offesa dovrà indicare l'URL

E' importante ribadire che se la persona offesa non è in grado di produrre la copia della pagina web o l'URL, nessun tipo di accertamento sarà possibile.

Infine occorre ricordare che la stessa persona offesa potrà richiedere formalmente al gestore la rimozione del contenuto illecito.

□ ALTRO REATO INFORMATICO

Trattasi di ipotesi residuali[31], allo stato di scarsa verificazione:

art. 615-*quater* c.p.	(detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)
art. 615-*quinquies* c.p.	(diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico)
art. 617-*bis* c.p.	(installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche)
art. 617-*ter* c.p.	(falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche)
art. 617-*quater* c.p.	(intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)
art. 617-*quinquies* c.p.	(installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)
art. 617-*sexies* c.p.	(falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)
art. 635-*bis* c.p.	(danneggiamento di informazioni, dati e programmi informatici)
art. 635-*ter* c.p.	(danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da un altro ente pubblico o comunque di pubblica utilità)
art. 635-*quater* c.p.	(danneggiamento di sistemi informatici e telematici)
art. 635-*quinquies* c.p.	(danneggiamento di sistemi informatici e telematici di pubblica utilità)
art. 640-*quinquies* c.p.	(frode informatica del soggetto che presta servizi di certificazione di firma elettronica)

[31] E **sempre che non si tratti di reato attinente la pedopornografia *online*** (in relazione alla quale sarà competente il diverso pool della Procura di Milano, III dipartimento),