SLS LAWYERS

LE TRUFFE INFORMATICHE

PRINCIPALI MODALITÀ E STRUMENTI DI TUTELA

E-BOOK

LE TRUFFE INFORMATICHE
PRINCIPALI MODALITÀ E STRUMENTI DI TUTELA

INDICE

3 Considerazioni preliminari

4 La disciplina giuridica

6 Le principali tipologie di truffe informatiche

8 Come proteggersi e cosa fare se si è stati truffati

10 Conclusione

E-BOOK

Considerazioni preliminari

La diffusione delle tecnologie informatiche e, più in generale, la progressiva digitalizzazione delle attività quotidiane hanno profondamente modificato anche le modalità attraverso le quali vengono perpetrate le truffe.

Acquistare un bene, effettuare un pagamento, gestire il proprio conto corrente, comunicare con una banca o con un ente pubblico sono oggi attività che possono essere svolte interamente online. Questa evoluzione ha indubbiamente prodotto importanti vantaggi in termini di rapidità e accessibilità dei servizi, ma ha anche creato nuove opportunità per chi intende realizzare condotte fraudolente. Pensiamo a un messaggio SMS che sembra provenire dalla propria banca, una telefonata effettuata da un presunto operatore dell'istituto di credito, un'e-mail apparentemente inviata da un ente pubblico o un annuncio pubblicato su un sito di compravendita: sono tutti fatti che possono essere sufficienti per indurre una persona a fornire credenziali, codici di sicurezza, dati personali o a effettuare un pagamento!

La peculiarità di questa tipologia di truffe che "sfruttano" la tecnologia non soltanto per realizzare l'illecito ma anche per manipolare la vittima e indurla a compiere operazioni in danno del proprio patrimonio, le rende particolarmente insidiose anche a fronte del fatto che vengono perpetrate attraverso l'utilizzo di sistemi che l'utente ritiene "sicuri". Comprendere, dunque, le principali tecniche utilizzate dai truffatori e conoscere le regole fondamentali di sicurezza rappresenta un utile strumento di difesa.

Lo scopo di questo breve elaborato è quello, passando per la sintetica esposizione delle norme giuridiche che regolano la specifica tipologia delittuosa, di "mettere in guardia" l'utente circa le principali tipologie di truffe informatiche e renderlo edotto sia sulle strategie da utilizzare per potersi tutelare, sia sugli eventuali rimedi.

Buona lettura!

La disciplina giuridica

Nel nostro ordinamento non esiste un'unica fattispecie penale ricomprendente tutte le frodi commesse attraverso internet o mediante strumenti tecnologici.

La qualificazione giuridica della condotta dipende dalle concrete modalità con cui il fatto viene realizzato e, soprattutto, dal ruolo che assume il sistema informatico nel meccanismo fraudolento. Le disposizioni alle quali occorre fare riferimento sono:

• **l'art. 640 del Codice Penale, che disciplina il reato di truffa.**

Tale norma prende in considerazione la "fattispecie tradizionale" attraverso la quale viene sanzionato il comportamento di chi, mediante artifici o raggiri, induce un'altra persona in errore e, sfruttando tale errore, procura a sé o ad altri un ingiusto profitto, causando un danno alla vittima.
L'elemento caratterizzante della truffa è quindi rappresentato dall'inganno.

Il soggetto agente costruisce una situazione falsa, apparentemente credibile, che induce la vittima a compiere un determinato comportamento. Quest'ultimo può consistere per esempio, nella consegna di denaro, nell'effettuazione di un pagamento, nella comunicazione di informazioni riservate o nel compimento di un atto che produce una conseguenza economicamente pregiudizievole;

• **l'art. 640 *ter* del Codice Penale, che disciplina il reato di frode informatica**.

Tale articolo, rispetto al precedente art. 640, prende in considerazione una modalità di aggressione differente, nella quale la condotta fraudolenta incide direttamente su un sistema informatico o telematico, oppure sui dati, sulle informazioni o sui programmi contenuti al suo interno.

La differenza tra le sopracitate due fattispecie delittuose sostanzialmente attiene al diverso destinatario dell'inganno.

Nella truffa tradizionale il soggetto che viene tratto in errore è una persona. Il criminale manipola la sua percezione della realtà e la induce a compiere un atto dannoso. Nella frode informatica, invece, la condotta fraudolenta è diretta nei confronti del sistema informatico o dei dati in esso contenuti, attraverso un'alterazione del suo funzionamento o un intervento privo di diritto.

La disciplina penale deve quindi essere applicata tenendo conto delle caratteristiche concrete della condotta, senza considerare automaticamente qualsiasi frode commessa online come una "frode informatica" in senso tecnico.

Inoltre, il quadro normativo si è evoluto per tenere conto delle nuove modalità attraverso le quali vengono commessi questi reati. Lo stesso art. 640 *ter* c.p. contempla specifiche ipotesi aggravate, attribuendo particolare rilevanza, tra l'altro, alle condotte che determinano un trasferimento di denaro, di valore monetario o di valuta virtuale, così come quelle caratterizzate dal furto o dall'indebito utilizzo dell'identità digitale.

E infatti, proprio l'identità digitale costituisce uno degli elementi maggiormente esposti alle frodi: credenziali di accesso, indirizzi e-mail, numeri di telefono, profili social e strumenti di autenticazione possono diventare vere e proprie "chiavi" attraverso le quali il criminale riesce ad assumere l'apparente identità della vittima o ad accedere ai suoi servizi.

Inoltre, dal punto di vista normativo, per completezza, meritano una menzione:

- il **D.lgs.vo n. 11/2010**, che prevede specifiche regole in materia di operazioni non autorizzate e di responsabilità del prestatore di servizi di pagamento;
- la disciplina europea in materia di servizi di pagamento e sicurezza delle transazioni elettroniche.

Su tali fronti particolare rilievo assume il principio dell'autenticazione forte del cliente, attraverso il quale si cerca di garantire che l'operazione sia effettivamente riconducibile al titolare dello strumento di pagamento. L'autenticazione forte si fonda, nei casi previsti dalla normativa, sull'utilizzo di almeno due elementi appartenenti a categorie differenti, riconducibili alla conoscenza, al possesso o all'inerenza del cliente.

Dopo questo sintetico *excursus* giuridico, esaminiamo ora dal punto di vista "pratico" le principali tipologie di truffe informatiche e i possibili strumenti di tutela.

Le principali tipologie di truffe informatiche

Le tecniche utilizzate dai criminali informatici sono in continua evoluzione, anche se molte di esse si fondano su uno schema ricorrente, ossia quello di ottenere la fiducia della vittima, creare un senso di urgenza e indurla a compiere un'azione che normalmente non avrebbe effettuato.

Le più frequenti tipologie di truffe informatiche sono:

a) **PHISHING:** consiste nell'invio di comunicazioni fraudolente, generalmente tramite e-mail, finalizzate a indurre il destinatario a fornire informazioni riservate. Il messaggio può apparentemente provenire da una banca, da un'azienda, da un ente pubblico o da un servizio online utilizzato abitualmente dalla vittima. Spesso il destinatario viene invitato a cliccare su un collegamento e ad accedere a una pagina Internet che riproduce graficamente quella dell'organizzazione autentica. Una volta inserite le credenziali, queste vengono raccolte dal truffatore. Il phishing può quindi rappresentare il primo passaggio di una frode più complessa, finalizzata successivamente all'accesso, per esempio, al conto corrente o all'utilizzo fraudolento dell'identità digitale.

b) **SMISHING:** è una variante del phishing realizzata attraverso SMS o altri sistemi di messaggistica. Un esempio ricorrente è il messaggio che informa la vittima della necessità di confermare un pagamento, aggiornare i dati bancari, bloccare una presunta operazione sospetta.

   Il messaggio contiene normalmente un link che conduce a una pagina fraudolenta.

   La pericolosità dello smishing deriva anche dalla maggiore immediatezza del mezzo utilizzato, ossia un SMS ricevuto sul proprio telefono che può apparire più credibile e urgente rispetto a un'e-mail.

c) **VISHING:** consiste nell'utilizzo della telefonata come strumento di inganno. Il truffatore può presentarsi come operatore della banca, appartenente alle forze dell'ordine, tecnico informatico, addetto alla sicurezza. La vittima viene informata dell'esistenza di un problema e invitata a fornire codici, credenziali o informazioni personali oppure a effettuare determinate operazioni. Una tecnica frequentemente utilizzata consiste nel creare una situazione di emergenza: "è stato disposto un bonifico", "il suo conto è sotto attacco", "deve autorizzare immediatamente il blocco dell'operazione".

   Lo scopo dei truffatori è quello di impedire alla vittima di riflettere e verificare autonomamente la veridicità della richiesta.

d) **SPOOFING:** si indicano con tecniche attraverso le quali il truffatore manipola determinati elementi identificativi della comunicazione per farla apparire proveniente da un soggetto legittimo. Può riguardare, ad esempio, il numero telefonico visualizzato sul dispositivo o l'indirizzo apparente del mittente di una comunicazione.

   La vittima può quindi ricevere una telefonata che sembra provenire dalla propria banca, oppure un messaggio inserito all'interno della stessa conversazione nella quale ha ricevuto in precedenza comunicazioni autentiche.

e) **TRUFFE SUI MARKETPLACE:** il truffatore pubblica un annuncio relativo a un prodotto particolarmente conveniente, chiedendo il pagamento anticipato e interrompendo successivamente ogni comunicazione.

   In altri casi invia alla vittima un falso link per ricevere il pagamento, con l'obiettivo di ottenere i dati della carta o le credenziali bancarie.

f) **BUSINESS EMAIL COMPROMISE:** riguardano soprattutto imprese e professionisti. Il truffatore riesce ad accedere a una casella di posta elettronica, oppure a simulare le comunicazioni di un soggetto con cui l'impresa intrattiene rapporti commerciali. La vittima può ricevere, ad esempio, una richiesta apparentemente proveniente da un fornitore, contenente nuove coordinate bancarie alle quali effettuare il pagamento di una fattura. Il pagamento viene quindi eseguito regolarmente, ma su un conto controllato dal truffatore.

Quelle sopraelencate sono solo una parte delle molteplici tipologie di truffe informatiche che, peraltro, sono destinate a diventare sempre più insidiose anche a seguito della diffusione degli strumenti di intelligenza artificiale che consente agevolmente di alterare e/o creare immagini, registrazioni vocali e video.

A questo punto sorgono spontanee due domande: come ci si può proteggere? Cosa fare se si è stati truffati?

Come proteggersi e cosa fare se si è stati truffati

Come esposto nel precedente paragrafo, nella maggior parte delle frodi informatiche il criminale cerca di ottenere dalla vittima un comportamento "impulsivo" (cliccare immediatamente su un link, fornire un codice, autorizzare un pagamento o comunicare una password).

La prevenzione quindi costituisce sicuramente il miglior strumento di difesa!

Basta poco!

È importantissimo per proteggersi ricordare che:

a) **non bisogna mai utilizzare i link contenuti all'interno di e-mail / sistemi di messaggistica, come per esempio SMS, WhatsApp e similari:** quando si riceve un messaggio relativo a un conto bancario, a una carta, a una spedizione o ad un servizio online, è opportuno evitare di utilizzare il link contenuto nella comunicazione. È preferibile aprire autonomamente l'applicazione ufficiale o digitare manualmente l'indirizzo del sito nel browser;

b) **non bisogna mai comunicare codici e credenziali:** password, PIN, codici OTP e altri codici di autenticazione sono dati personali che devono essere mantenuti riservati.

   Gli istituti di credito normalmente non chiedono telefonicamente al cliente di comunicare il proprio codice di sicurezza con il pretesto di "bloccare" una frode. Anche quando l'interlocutore conosce alcune informazioni personali della vittima, non bisogna considerare automaticamente autentica la comunicazione;

c) **è necessario verificare sempre l'identità dell'interlocutore:** in caso di telefonata sospetta è preferibile interrompere la conversazione e contattare autonomamente l'ente interessato utilizzando un numero ufficiale.

   Lo stesso principio vale per le richieste ricevute tramite e-mail o messaggistica. Una richiesta urgente di pagamento, modifica delle coordinate bancarie o trasferimento di denaro deve essere sempre verificata attraverso il "canale ufficiale";

d) **è necessario utilizzare sistemi di autenticazione sicuri:** è importante, quando disponibile, utilizzare l'autenticazione a più fattori e tenere sempre aggiornati i dispositivi e le credenziali di accesso alle applicazioni di home banking;

e) **è consigliabile limitare le informazioni pubblicate online:** le informazioni pubblicate sui social network possono essere utilizzate dai truffatori per rendere più credibili le loro comunicazioni. Dati relativi alla famiglia, al lavoro, alle abitudini personali o ai viaggi possono infatti essere utilizzati per costruire messaggi estremamente personalizzati;

f) **bisogna prestare attenzione a frasi come** "devi agire immediatamente", "il tuo conto verrà bloccato", "devi autorizzare ora il pagamento" o "non interrompere la telefonata" devono indurre a fermarsi e verificare.

✳

Invece, quando la frode si è già verificata la tempestività è fondamentale!

È importantissimo:

- contattare immediatamente il proprio istituto di credito segnalando l'accaduto e chiedendo il blocco immediato degli strumenti eventualmente compromessi e, quando possibile, delle operazioni ancora revocabili o recuperabili;

- modificare immediatamente le password che potrebbero essere state compromesse e verificare l'eventuale accesso abusivo alla propria posta elettronica, ai social network e agli altri account;
- conservare tutte le prove disponibili. A titolo esemplificativo: SMS, e-mail, eventuali conversazioni tramite WhatsApp o altri sistemi di messaggistica;
- denunciare tempestivamente l'accaduto alle autorità competenti, descrivendo i fatti nel modo più preciso possibile e allegando la documentazione disponibile.

Conclusione

Le truffe informatiche rappresentano oggi una delle forme più insidiose di aggressione al patrimonio, non soltanto per la rapidità con cui possono essere realizzate, ma soprattutto perché sfruttano una caratteristica tipica della società digitale, ossia, la difficoltà di distinguere, in determinate situazioni, ciò che è autentico da ciò che è costruito artificialmente per apparire autentico. Naturalmente, la prevenzione non elimina completamente il rischio. Può accadere che anche una persona attenta e consapevole cada vittima di un raggiro particolarmente sofisticato. In questi casi è altrettanto importante sapere come reagire. La tempestività può fare la differenza: contattare immediatamente la banca o l'intermediario, bloccare gli strumenti di pagamento eventualmente compromessi, modificare le credenziali, mettere in sicurezza gli account e conservare ogni elemento utile alla ricostruzione dell'accaduto sono attività che non devono essere rimandate.

Inoltre, quando la truffa ha determinato una perdita economica, quando sono stati utilizzati indebitamente strumenti di pagamento, quando sono state sottratte credenziali o identità digitali, oppure quando occorre contestare un'operazione nei confronti di una banca o di un altro intermediario, è opportuno anche rivolgersi tempestivamente a un professionista legale, che possa valutare concretamente il caso, individuare gli strumenti di tutela più adeguati e assistere la persona nelle eventuali iniziative necessarie per cercare di recuperare le somme perdute e far valere i propri diritti, incluso il risarcimento del danno derivante dalla abusiva intromissione nella propria situazione di vita.

SLS
LAWYERS

MONZA

Via Vittorio Emanuele II, 26
tel. 039 2304417
fax 039 2301588

MILANO

Via Rugabella, 1
tel. 02 89011611
fax 02 89012202

WWW. SLS-LAWYERS.EU

segreteria@sls-lawyers.eu

SLS – Lawyers

design _ Mazzantini.com