PREVENZIONE E CONTRASTO AI FENOMENI DI CRIMINALITÀ INFORMATICA CONTRO LE FRODI ONLINE

«LA SPECIALITÀ...IN RAGIONE DEGLI ELEVATI LIVELLI DI COMPETENZA E CAPACITÀ INVESTIGATIVA...SVOLGERÀ...ATTIVITÀ DI PREVENZIONE E CONTRASTO AI FENOMENI DI CRIMINALITÀ INFORMATICA CHE IMPIEGANO PARTICOLARI TECNICHE DI HACKING, TECNOLOGIE SOFTWARE O HARDWARE PER CARPIRE, RIPRODURRE ED UTILIZZARE FRAUDOLENTEMENTE IDENTITÀ DIGITALI, CODICI DI UTILIZZO DI SERVIZI BANCARI ONLINE E DI CARTE DI PAGAMENTO NELLE TRANSAZIONI ELETTRONICHE...»

I reati più ricorrenti nel contrasto al crimine finanziario di tipo informatico sono: la truffa (art. 640 c.p.), la frode informatica (art. 640-ter c.p.), il furto d'identità digitale (sostituzione di persona, art. 494 c.p.), l'accesso abusivo a sistema informatico (art. 615-ter c.p.), la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.), la ricettazione (art. 648 c.p.) il riciclaggio (art. 648-bis c.p.), l'indebito utilizzo di carte di credito (art. 55 del decreto legislativo 231/2007).

Di seguito, le fattispecie più ricorrenti in cui tali reati si manifestano.

1) **Truffe in ambiente e-commerce**

Sono truffe relative alla vendita di beni e servizi su piattaforme di commercio elettronico.

Si distinguono in:

Truffe «da annuncio»: Il truffatore sfrutta portali di commercio elettronico ufficiali e collaudati (ad es. Ebay, Subito.it, Annunci, ecc…) per inserire annunci truffaldini

Truffe «da sito»: il truffatore crea portali internet di vendita interamente falsi.

PREVENZIONE E CONTRASTO AI FENOMENI DI CRIMINALITÀ INFORMATICA CONTRO LE FRODI ONLINE

2) **Il Phishing**

Il Phishing è una particolare tipologia di truffa realizzata sulla rete internet, principalmente attraverso l'invio di messaggi di adescamento via posta elettronica, spesso apparentemente provenienti da pubbliche amministrazioni, aziende erogatrici di servizi pubblici, istituti finanziari ed importanti imprese commerciali.
Il messaggio invita ad aprire un link o un allegato malevolo.
Una volta cliccato sul link, esso installa sulla macchina attaccata un virus informatico, che permette l'assunzione del controllo della macchina, il furto dei dati, l'attivazione di webcam o microfoni, la disabilitazione di protezioni ed antivirus

3) **Attacchi «man in the mail»: B.E.C. e CEO Fraud**

Attraverso la compromissione di una casella di posta elettronica, oppure tramite tecniche di social engineering, l'hacker apprende che è in corso una corrispondenza elettronica di carattere commerciale tra due soggetti (B.E.C. - Business e-mail compromise). Assunta l'identità digitale di una delle parti, il criminale richiede pagamenti all'altra parte su conti correnti appositamente creati, spesso allocati all'estero.
Una variante di tale schema vede la sostituzione di persona consumarsi ai danni di manager di alto livello nella gerarchia di un'azienda o di un'Istituzione (CEO Frauds): il falso manager induce un soggetto dell'organigramma aziendale, dotato di poteri di spesa, a disporre trasferimenti di denaro, col pretesto di dover adempiere ad un ordine gerarchico. Anche in questo caso, i conti corrente sui quali confluisce il provento illecito risultano spesso allocati all'estero.

PREVENZIONE E CONTRASTO AI FENOMENI DI CRIMINALITÀ INFORMATICA CONTRO LE FRODI ONLINE

4) **Le violazioni dei sistemi di Home Banking**

Tale tipologia rati prevede la violazione dei sistemi di home banking appartenenti ad ignari correntisti, per poter successivamente disporre trasferimenti di denaro.
La violazione può avvenire attraverso attacco informatico diretto alla piattaforma bancaria. Il più delle volte, tuttavia, essa avviene grazie al previo ottenimento dei codici di accesso alla piattaforma stessa da parte del truffatore. Questi entra in possesso dei codici di accesso nei modi più vari (virus informatici, intercettazioni illegali, acquisto delle credenziali sul mercato nero virtuale, semplice imprudenza da parte del titolare)

5) Il riciclaggio di denaro attraverso il web: il fenomeno dei **Money Mules**

Il Money Mule (Mulo di denaro) è una soggetto utilizzato, all'interno di uno schema criminale, per conseguire, ricettare o riciclare il provento di un reato.
Accade spesso che soggetti economicamente o socialmente deboli, accettino dietro pagamento di attivare a proprio nome conti correnti o altri rapporti finanziari, per poi mettere tali rapporti a disposizione di sodalizi criminali.
Tuttavia, in alti casi, i criminali riescono attraverso il web a reclutare inconsapevoli muli di denaro. Ciò avviene, nella maggior parte dei casi, attraverso la pubblicazione di false offerte di lavoro via internet: la vittima viene indotta con l'inganno ad aprire conti correnti o altri rapporti finanziari, in virtù della falsa promessa di un «lavoro» consistente nel ricevere somme di denaro su tali conti, da movimentare successivamente.

PREVENZIONE E CONTRASTO AI FENOMENI DI CRIMINALITÀ INFORMATICA CONTRO LE FRODI ONLINE

6) **Furto di dati e codici personali attraverso siti-clone**

Mediante la predisposizione di pagine web del tutto somiglianti a quelle autentiche di banche, piattaforme di pagamento e grandi aziende, il truffatore induce la vittima ad inserire i propri codici personali e bancari, per poi appropriarsene.

7) **I Black Market e Darkweb**

I Black Market costituiscono oggi la nuova frontiera del crimine finanziario informatico, su cui si concentra l'impegno delle forze di Polizia di tutto il mondo. All'interno delle piattaforme illecite di commercio elettronico, ospitate nel dark web, avvengono le transazioni e gli scambi più intensi e lucrosi per il mondo criminale. Uno spazio per larga parte inesplorato, all'interno del quale si cela ogni genere di traffico illecito: dalle armi clandestine alle sostanze stupefacenti, dai documenti contraffatti al materiale pedopornografico, dalle carte di pagamento clonate a password e codici di accesso personali di migliaia di utenti.

8) **Le Botnet**

Una botnet, nel linguaggio informatico, rappresenta una rete di centinaia di migliaia di computer, che vengono infettati dai criminali informatici allo scopo di assumerne il controllo all'insaputa dei legittimi proprietari; successivamente, tali computer possono essere manovrati dai criminali ed utilizzati come veicolo per la commissione di innumerevoli reati informatici su larga scala, quali il furto di dati personali, password, numeri di carte di credito, indirizzi, numeri di telefono e dati sensibili.

PREVENZIONE E CONTRASTO AI FENOMENI DI CRIMINALITÀ INFORMATICA CONTRO LE FRODI ONLINE

9) **I BitCoin e le Criptovalute: Frodi e riciclaggio**

Le cosiddette “valute virtuali”, oggetto di crescente diffusione, sono utilizzate sempre più come mezzo di scambio per l’acquisto di beni e servizi. Esse possono essere trasferite, conservate e negoziate elettronicamente; non sono emesse da banche centrali o da autorità pubbliche; non costituiscono moneta legale né sono assimilabili alla moneta elettronica. Le operazioni effettuate con valute virtuali avvengono prevalentemente on line, fra soggetti che possono operare in Stati diversi, spesso anche in Paesi o territori a rischio . Tali soggetti non sono facilmente individuabili ed è agevolato l’anonimato sia di coloro che operano in rete, sia dei reali beneficiari delle transazioni, circostanza che può talvolta suggerirne l’utilizzo per scopi illeciti di frode, finanziamento illecito e riciclaggio.