# Hacker Highschool
## SECURITY AWARENESS FOR TEENS

# LEZIONE 12
# INTERNET: ETICA E LEGALITÀ

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

# “License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.



# Informazioni sulla licenza d’uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e liberamente disponibile al pubblico, secondo i termini e le condizioni di ISECOM. Per comprendere le nostre condizioni di utilizzo, o acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE di questo sito web.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

# Indice dei contenuti

# Contributors

Francisco de Quinto, Piqué Abogados Asociados

Jordi Saldaña, Piqué Abogados Asociados

Jaume Abella, Enginyeria La Salle (URL) – ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

## Per la versione in lingua italiana:

Raoul Chiesa (ISECOM)

Doriano Azzena (centro CSAS del progetto Dschola IPSIA Castigliano - Asti )

Sophia Danesino (centro CSAS del progetto Dschola ITIS Peano – Torino )

Nadia Carpi (centro CSAS del progetto Dschola ITIS Peano – Torino )

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

mediaservice.net
CORPORATE SECURITY & IMAGE

# 12.1. Introduzione

Le nuove tecnologie, mentre sviluppano un nuovo paradigma che invade tutti gli ambiti delle attività umane, influenzano anche l'aspetto oscuro di tali attività: comportamenti criminali di individui e di gruppi organizzati.

Per questo motivo abbiamo riservato l'ultima lezione di HHS per analizzare vari aspetti che si riferiscono alla legalità e all'etica di internet, analizzando alcuni comportamenti che potrebbero condurre a crimini e alle possibili conseguenze.

# 12.2. Crimini transnazionali e diritto nazionale

Come già evidenziato, l'introduzione delle nuove tecnologie può influenzare i comportamenti criminosi d'individui e di gruppi organizzati. Ci sono due principali caratteristiche attraverso le quali le Tecnologie dell'Informazione e della Comunicazione (in seguito TIC) si possono correlare alle attività criminose:

1. Le tecnologie offrono la possibilità di rinnovare i modi tradizionali di delinquere. Esistono attività illegali contemplate nel codice penale, che sono perpetrate in modi nuovi. Ad esempio citiamo il riciclaggio di capitale e la pornografia minorile.
2. Il contenuto innovativo delle TIC ha favorito la comparsa di nuovi tipi di crimine che a causa della loro novità stanno per essere contemplati dalla legislazione penale di numerosi paesi. Ad esempio la distribuzione di spam e di virus.

Un'altra caratteristica delle TIC che deve essere evidenziata è la localizzazione territoriale che influenza il particolare contesto geografico, ma senza dubbio anche altri paesi.

L'attuale diritto presenta una chiara vocazione territoriale che si sostanzia in GIURISDIZIONE COMPETENTE e LEGGE APPLICABILE.

In altre parole possiamo affermare che le TIC sono globali e senza confini, mentre le leggi e i tribunali sono territoriali e limitati a uno specifico stato o territorio. Inoltre il fenomeno della globalizzazione genera un disorientamento ancora più marcato di quanto possa sembrare. Una comunicazione on-line tra un utente in Torino e un sito web allocato presso un provider situato in California può attraversare più di una decina di host situati geograficamente in luoghi differenti. La diversità di indirizzi e nazioni ci suggerisce un quesito: quale legge e di quale paese applicare in caso di controversie?

Vale la pena citare l'accordo sul Crimine informatico (cyber-crime) siglato nel Consiglio Europeo il 23 Novembre 2001 a Budapest da 30 paesi tra cui figurano i membri della Comunità Europea, gli Stati Uniti d'America, il Canada, il Giappone, e il Sudafrica. L'accordo instaura il PRINCIPIO DI TERRITORIALITA' per definire la giurisdizione competente. La firma dell'accordo è il risultato di quattro anni di lavoro che hanno prodotto un documento composto di 48 articoli organizzati in quattro categorie:

1. Infrazioni contro la confidenzialità
2. Falsificazione e frode informatica
3. Infrazioni che si riferiscono ai contenuti
4. Violazioni della proprietà intellettuale

Una volta descritte le complesse regolamentazioni e sanzioni delle attività criminose su internet, deve essere ricercato il consenso su tre principali difficoltà:

1. **CONFLITTI DI GIUIRISDIZIONE.** Elezione del tribunale competente per giudicare un crimine multinazionale e transnazionale. Il problema non è risolto da nessuno dei sistemi giudiziari noti.
2. **CONFLITTI DI LEGISLAZIONE.** Una volta definito il tribunale si tratta di scegliere quale legge applicare al particolare caso. Ancora una volta sottolineiamo che i tradizionali criteri legislativi non sono adatti ai confini virtuali di un reato telematico.
3. **APPLICAZIONE DELLA SENTENZA.** Una volta che il tribunale ha emesso la sentenza, essa deve essere applicata prevedibilmente in un paese diverso da quello del tribunale che l'ha emessa. E' di conseguenza necessario un compromesso internazionale per riconoscere ed accettare le sentenze emesse. Questa difficoltà è tuttavia più complessa da risolvere delle due precedenti.

Queste difficoltà sono state chiaramente dimostrare nel recente episodio di un hacker in Russia, il quale ha violato diversi sistemi statunitensi e fu invitato presso una falsa azienda statunitense per un colloquio.

Durante il colloquio, dimostrò le sue capacità effettuando azioni di hacking presso la sua stessa rete in Russia. Alla fine risultò che il colloquio fu tenuto dall'FBI stessa e lui fu arrestato. L'FBI installò sniffers sul computer utilizzato durante il colloquio, i quali portarono al computer dell'hacker - sito in Russia - and scaricarono le prove che furono utilizzate per condannarlo.

Ma ci sono comunque molti punti irrisolti:

- Era legale per l'FBI esaminare il contenuto di un computer sito in Russia, senza ottenere un'autorizzazione dal governo Russo ?
- Invitando l'hacker negli Stati Uniti, l'FBI ha evitato di richiedere l'estradizione negli Stati Uniti. Questo fu legale ?
- Poteva il governo degli Stati Uniti condannare una persona per crimini che erano tecnicamente commessi sul territorio sovietico ?

Infine, l'hacker fu condannato negli Stati Uniti in quanto utilizzò un Proxy Server sito negli Stati Uniti per lanciare alcuni attacchi. Ha passato solamente 4 anni in prigione ed ora vive e lavora negli Stati Uniti.

**Esercizio:**

Conduci una discussione alternativa del tipo "White-hat / Black-hat" per almeno una delle seguenti domande (esame di un computer in territorio straniero; invito o trappola per evitare l'estradizione; condanna per crimini informatici commessi contro un paese da territorio straniero).

1. Innanzitutto, fate focalizzare gli studenti su - e fate loro elencare - i motivi per i quali l'argomento scelto rientrava probabilmente nella legalità.

2. Successivamente, invertite l'ottica di analisi e fate loro focalizzare ed elencare perchè l'argomento scelto era probabilmente illegale.

3. Dopo queste discussioni completamente separate, provate a vedere se la classe riesce a raggiungere una decisione comune.

Nota - queste domande sono interessanti per un dibattito, un confronto. Non vi sono "risposte esatte", ed i governi stanno ancora lavorando per arrivare ad un consenso su questa ed altre tematiche relative alla natura internazionale di queste crimini. Questo eservizio è puramente per esaminare e pensare in modo critico alla tematica dei crimini via Internet, così come alla formulazione di argomentazioni logiche per la creazione di un'opinione relative a questa tipologia di crimini.

# 12.3. Delitti che si riferiscono alle TIC

La classificazione dei comportamenti criminali è uno dei principi fondamentali dei sistemi penali; per questo motivo molti paesi devono pensare a introdurre modifiche nel codice penale. In Italia i reati informatici e telematici sono contemplati dal Codice Penale (vedi in seguito).

Fra l'altro possiamo classificare le potenziali azioni criminose nelle seguenti sezioni:

1. Manipolazione di dati e informazioni contenuti in file su computer o su altri dispositivi informatici.
2. Accesso o uso di dati senza autorizzazione.
3. Inserimento di programmi o sottoprogrammi in altri computer allo scopo di cancellare o modificare dati o applicazioni.
4. Utilizzo di computer e di applicazioni appartenenti ad altri senza esplicita autorizzazione allo scopo di procurare benefici a se stesso e/o danni ad altri.
5. Uso del computer con intenzioni fraudolente.
6. Violazione del codice sulla privacy (D.lgs. 30/06/2003 n. 196) attraverso l'accesso, l'uso e l'elaborazione di dati personali senza esplicito incarico.

Il delitto tecnologico si caratterizza per le difficoltà nello scoprirlo, provarlo, perseguirlo. Le vittime a volte preferiscono non denunciarlo per evitare l'eventuale allarme sociale e il probabile discredito derivante dall'implicita ammissione dell'esistenza di falle nel sistema di sicurezza informatico; i perseguitati scelgono di subire le conseguenze del delitto e adottare strategie per prevenire nel futuro il ripetersi di tali episodi. Questa situazione ostacola il riconoscimento del numero di delitti commessi e l'adeguata pianificazione delle misure legali preventive.

Tutto ciò è complicato dai rapidi cambiamenti delle tecnologie. Tuttavia, le leggi stanno cambiando e a disposizione dei giudici sono introdotti sempre più strumenti legali, giuristi ed avvocati lavorano per punire i crimini che si riferiscono alle TIC.

Analizziamo di seguito alcuni specifici delitti relativi alle TIC contemplati dal Codice Penale italiano:

1. Accesso abusivo ad un sistema telematico od informatico Art. 615 ter.
2. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici Art. 615 quater.
3. Diffusione di programmi diretti a danneggiare od interrompere un sistema informatico Art. 615 quinquies.
4. Violazione, sottrazione e soppressione di corrispondenza Art. 616.

5. Intercettazione, impedimento, od interruzione illecita di comunicazioni informatiche o telematiche Art. 617 quater.
6. Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche e telematiche Art. 617 quinquies.
7. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche Art. 617 sexies.
8. Frode informatica: Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura per sé o ad altri un ingiusto profitto con danno altrui commette il reato. Art.640 ter.
9. Diritto d'autore: Copie illegali e diffusione di materiali copy-righted, letterari, artistici, scientifici con qualsiasi mezzo senza l'autorizzazione di coloro che ne hanno la proprietà intellettuale o dei loro rappresentanti**.** Art. 30 e 32-bis

***Esercizio***:

1. Scegli uno degli argomenti sopra elencati e conduci una delle seguenti ricerche:

- Trova un caso legale che possa essere classificato come tipologia di crimine scelto.
- C'è stato un giudizio legale e, se c'è stato, è stata applicata una sentenza ?
- Perchè gli autori hanno commesso questo crimine ?

In merito alla proprietà intellettuale, possono le seguenti azioni essere considerate come un crimine?

- Fotocopiare un libro nella sua interezza
- Copiare musica da un CD che non abbiamo acquistato
- Effettuare una copia di un CD musicale che abbiamo acquistato
- Scaricare musica MP3, o fim in DIVX da Internet
- Cosa diresti se si trattasse della tua musica o film dai quali non ottieni le royaltes che ti aspetti ? Cosa diresti se si trattasse di una tua opera d'arte, che altri copiano menzionandosi tra gli autori ?

# 12.4. Prevenzione dei delitti e tecnologia doppio uso

L'unico modo affidabile per prevenire le aggressioni criminali nel campo delle TIC è quello di applicare ragionevolmente le misure di sicurezza che sono state illustrate nelle lezioni precedenti di HHS. E' anche estremamente importante che l'applicazione di tali misure avvenga in una forma che per noi diventi praticamente impossibile incorrere in comportamenti dubbiosi o addirittura delittuosi. Sottolineiamo che le tecnologie possono avere molteplici usi e che alcune tecniche usate per la sicurezza possono, simultaneamente generare attività criminose. Ciò prende il nome di TECNOLOGIE DAL DOPPIO USO, i cui massimi esponenti sono la crittografia e le tecniche per intercettare la comunicazione

elettronica. Questa sezione descrive la realtà del fenomeno e le sue conseguenze allarmanti in tutti i livelli dell'attività umana, politiche, sociali, economiche, di ricerca.

### 12.4.1.1 Il sistema globale di monitoraggio: COMINT

Recentemente è stato creato il termine COMINT risultato dell'integrazione dei termini COMmunication e INTelligence e si riferisce all'intercettazione della comunicazione che è risultata dallo sviluppo dall'uso massiccio delle TIC.

COMINT rappresenta anche un'attività economica a fini di lucro che fornisce ai clienti, pubblici e privati, contenuti intelligenti "on-demand", in particolar modo nelle aree della diplomazia, economia, ricerca. Ciò ha significato il superamento dell'obsoleto schema di spionaggio militare con l'implementazione più o meno aperta delle nuove tecnologie per la raccolta e l'esame dei dati.

Gli esempi più rappresentativi delle tecnologie COMINT sono i sistemi "ECHELON" e "CARNIVORE" che analizziamo di seguito.

## 12.4.2. Il sistema "ECHELON"

Il sistema ha origine nel 1947, subito dopo la fine della II guerra mondiale, in un accordo fra UK e USA con chiari intenti militari e di sicurezza. I dettagli di questo accordo non sono ancora completamente noti. In seguito aderirono all'accordo Canada, Australia e Nuova Zelanda che operano come fornitori di informazioni e subordinati.

Il sistema lavora intercettando indiscriminatamente una gran quantità di comunicazioni, indipendentemente dai mezzi di trasporto e immagazzinamento, con particolare riferimento alle seguenti aree:

- Trasmissioni a larga banda (wideband e Internet).
- Comunicazioni telefoniche e facsimile via cavo: intercettazione dei cavi, compresi quelli sottomarini mediante navi opportunamente equipaggiate.
- Comunicazioni cellulari.
- Sistemi di riconoscimento della voce.
- Sistemi di riconoscimento biometrico come il riconoscimento facciale tramite filmati anonimi.

In seguito l'informazione ritenuta interessante è estratta secondo le finalità del sistema Echelon, con tecniche d'intelligenza artificiale per definire e applicare parole chiave (KEY WORDS).

Ognuno dei cinque paesi membri fornisce dizionari di parole chiave che sono introdotte nei dispositivi di intercettamento e agiscono come un filtro automatico. Logicamente le parole e i dizionari cambiano nel tempo in funzione degli interessi degli stati membri del sistema. Al principio Echelon aveva chiari scopi militari; col tempo è diventato un sistema duale; ufficialmente attivo per la prevenzione del crimine internazionale organizzato (terrorismo, traffico d'armi e di droga, dittature ecc.) ma con un'influenza che raggiunge l'economia globale e la politica commerciale delle imprese e delle zone di influenza economica.

Negli ultimi tempi Echelon ha operato come una struttura a stella con cinque punte in due principali aree. Entrambe le strutture appartengono alla NSA (National Security Agency): una

negli Stati Uniti, coincidente con il quartier generale a Fort Meade (Maryland) e l'altra in Inghilterra, al Nord dello Yorkshire, nota come Meanwith Hill.

I punti della stella sono occupati dalle stazioni di tracciamento (tracking) dei soci collaboratori:

- USA(2): Sugar Grove e Yakima.
- Nuova Zelanda (1): Wai Pai.
- Australia (1): Geraldtown.
- UK (1): Morwenstow (Cornwell).

Ce n'era una a Honk Kong che cessò di operare quando i territori furono ceduti alla Cina.

N.B.: per approfondimenti sull'argomento, si rimanda all'e-book - gratuito e liberamente scaricabile dalla rete Internet - "Le reti di controllo globale: un'analisi approfondita dei casi Echelon ed Enfopol" di Raoul Chiesa.

## 12.4.3. Il sistema "Carnivore"

Il secondo sistema globale di intercettamento e spionaggio è quello sponsorizzato dalla FBI ed è conosciuto come "CARNIVORE" con il dichiarato obiettivo di combattere il crimine organizzato e di rinforzare la sicurezza degli Stati Uniti. La potente tecnologia utilizzata, la versatilità di applicazione delle sue aree di ascolto e di attenzione ha favorito lo scontro tra il sistema "CARNIVORE", le organizzazioni politiche e i media di massa.

"CARNIVORE" è stato sviluppato nel 2000 ed è un sistema automatico che intercetta le comunicazioni internet basandosi su uno dei principi fondamentali della rete: il flusso dell'informazione avviene per gruppi di dati uniformi (pacchetti).

Il sistema è capace di intercettare i pacchetti di informazione; si suppone che ciò sia fatto a difesa della sicurezza nazionale e per rinforzare la lotta contro il crimine tecnologico organizzato.

Le organizzazioni per i diritti civili statunitensi hanno immediatamente denunciato un nuovo attacco alla privacy delle comunicazioni elettroniche. L'EPIC (Electronic Privacy Infomation Center) ha richiesto che un giudice federale ordini alla FBI di permettere l'accesso per ISP (internet provider) al sistema di vigilanza - al fine di garantire che il sistema sia utilizzato entro i limiti fissati dalla legge.

All'inizio di Agosto 2000 la Corte di Appello del distretto di Columbia respinse una legge che permetteva alla FBI di intercettare le comunicazioni ( in particolare i cellulari) senza dover chiedere la preventiva autorizzazione al giudice, per mezzo di un progetto della Commissione Federale delle Telecomunicazioni che cercava di obbligare le compagnie di telefonia mobile a installare dispositivi di tracciamento (tracking) in tutti i dispositivi mobili per ottenere la localizzazione automatica delle chiamate. Il costo di fabbricazione dei telefoni cellulari sarebbe aumentato del 45%.

Con questi due esempi si evidenziano le intenzioni della FBI di generare un sistema Echelon domestico operativo su internet e sulla telefonia cellulare, conosciuto come "CARNIVORE".

Il progetto è stato respinto da diversi Tribunali statunitensi e dal Congresso perché in questa versione iniziale trattasi di un'aggressione ai Diritti Civili dei cittadini Americani.

Il progetto si sta ripensando, almeno formalmente, includendo la preventiva autorizzazione del giudice come requisito per accettare i dati ottenuti (le informazioni) come prova in sede di dibattimento.

***Esercitazione 1***

Circola in internet una burla che si riferisce al sistema COMINT. La comprendiamo in questa lezione per stimolare la discussione di classe e per le implicazioni etiche e legali:

Un vecchio arabo musulmano iracheno domicilaito in Chicago da più di 40 anni desidera piantare patate nel suo giardino, però arare la terra è un lavoro troppo difficile per lui. Il suo unico figlio, Amhed, studia in Francia. Il vecchio uomo invia un messaggio e-mail al figlio spiegandogli il problema:

" Amhed, mi sento male perché quest'anno non sono capace di piantare le patate nel mio giardino. Sono troppo vecchio per arare il terreno. Se tu fossi qui tutti i miei problemi scomparirebbero. So che areresti per me il terreno. Con affetto papà."

Alcuni giorni dopo, arriva il messaggio di risposta del figlio:

"Padre: Per amor del cielo, non toccare il suolo del giardino. E' il posto dove nascondo … Con affetto Amhed."

La mattina seguente alle 4:00, improvvisamente arrivano agenti della polizia locale, FBI, CIA, RANGERS, MARINES, rappresentanti del Pentagono, che rimuovono il terreno alla ricerca di antrace, materiale per costruire bombe ecc. Non trovano nulla e se ne vanno.

Lo stesso giorno il vecchio uomo riceve un altro messaggio dal figlio:

"Padre: Certamente il terreno è pronto per piantare le patate. Ho fatto del mio meglio, date le circostanze. Con affetto Amhed."

**Esercitazione 2**

Con Internet cercate informazioni sui sistemi Echelon e Carnivore e sulle loro applicazioni alle reti e alle TIC nel vostro paese per rispondere alle seguenti domande:

1. Cosa significa il termine Echelon?
2. Quali elementi compongono il sistema Echelon?
3. Quali elementi formano il sistema Carnivore?
4. Cercate un esempio di controversia attribuita al sistema Echelon che si riferisce a personalità famose.
5. Cercate un esempio di applicazione del sistema Carnivore che si riferisce ad un terrorista universalmente noto.
6. Qual è la vostra opinione sulla legalità di tali sistemi?

# 12.5. Hacking etico (Ethical Hacking)

Abbiamo parlato di comportamenti criminali, crimini e sanzioni, tuttavia desideriamo evidenziare che essere un hacker non significa essere un delinquente.

Oggigiorno le aziende stanno assumendo i servizi dagli hacker etici (ethical hackers) per rilevare le vulnerabilità dei loro sistemi informatici e per migliorare le misure di difesa.

Gli hacker etici, con la loro conoscenza, aiutano a definire i parametri di difesa. Eseguono attacchi controllati, preventivamente autorizzati dalle organizzazioni, per verificare le difese dei sistemi; creano gruppi per imparare nuove tecniche d'attacco, exploit, vulnerabilità, ecc.

Come scrisse Sun Tzu nel suo libro "L'arte della guerra", "l'attacco è il segreto della difesa; la difesa è la pianificazione dell'attacco".

La metodologia dell'hacker etico si suddivide nelle seguenti fasi:

1. Pianificazione dell'attacco.
2. Accesso a Internet.
3. Test e esecuzione dell'attacco.
4. Analisi.
5. Valutazione e diagnosi.
6. Rapporto finale.

Uno strumento che gli hacker etici utilizzano è il manuale "OSSTMM - Open Source Security Testing Methodology Manual" (http://www.osstmm.org) . La metodologia indicata è adatta a testare qualsiasi sistema di sicurezza, dalle protezioni e porte alle telecomunicazioni via satellite, mobili ed ai satelliti. Il metodo è applicato ed usato dalle organizzazioni importanti come:

- Istituzioni finanziarie spagnole.
- Dipartimento del Tesoro degli Stati Uniti per testare le istituzioni finanziarie.
- US Navy & Air Force.
- Ecc.

**Esercizio**

- Cercate informazioni sull'hacking etico e sul suo ruolo nelle aziende che si occupano di sicurezza informatica.
- Cercate informazioni su OSSTMM e sulle metodologie.
- Cercate informazioni sulle certificazioni che si riferiscono all'hacking etico (ethical hacking).

# 12.6. Le dieci frodi più comuni su internet

Di seguito è elencato un sommario dalla Commissione commerciale federale degli Stati Uniti dei crimini più comuni su Internet a partire dal 2005.

1. Aste Internet: Acquisti in un "negozio virtuale" che offre una vasta scelta di prodotti e grandi affari. Dopo il pagamento, i consumatori ricevono un articolo più modesto di quanto promesso, o, più difettoso o non ricevono nulla.
2. Servizi di accesso a internet: i consumatori sono "intrappolati" in contratti di lunga durata per l'accesso a Internet o ad altro servizio, con notevoli penali per l'annullamento del contratto prima del termine.
3. Frode della carta di credito: falsificazione ed uso fraudolento della medesima.
4. Dialers: sostituire la connessione telefonica (dial-up) corrente, con un'altra a tariffazione maggiorata.
5. Web cramming: ottenere un sito web personale gratuito per un periodo di prova, in genere di 30 giorni, senza l'obbligo di continuare. Ai consumatori giungono gli addebiti in bolletta telefonica o in altro modo, anche senza il consenso a continuare il servizio dopo il periodo di prova.
6. Programmi di vendita multilivelli: Fate soldi con i prodotti ed i servizi che vendete, come pure quelli venduti alle persone che reclutate per partecipare al programma. I consumatori dicono che hanno comprato nei programmi, ma i loro clienti sono altri distributori, non il grande pubblico.
7. Viaggi e vacanze: Ottenere un viaggio meraviglioso con molti supplementi ad un prezzo da vero affare. Le agenzie forniscono sistemazioni e servizi di qualità inferiore a quanto pubblicizzato o addirittura nessun viaggio. Altre impongono spese nascoste o requisiti supplementari dopo che i consumatori hanno pagato.
8. Occasioni di affari: Attratto dalle promesse di facili guadagni molti consumatori hanno investito ed il risultato è stato un flop. Non c'erano prove sufficienti per sostenere le richieste di risarcimento delle somme investite.
9. Investimenti: Fate un investimento iniziale in un sistema "day trading" (compravendita di azioni in giornata a scopo speculativo) e realizzerete rapidamente grossi guadagni. Grandi profitti significano sempre grandi rischi. I consumatori hanno perso capitali in programmi che sostengono di potere predire il mercato con il 100% d'esattezza.
10. Sanità Prodotti e trattamenti: La pubblicità per i prodotti ed i trattamenti "miracolosi" convincono i consumatori che i loro problemi di salute possono trovare una soluzione. Le persone con malattie serie che ripongono le loro speranze nella forza di queste offerte ritardano il ricorso alle cure di cui necessitano realmente.

**Esercizio**

Pensate alle seguenti domande e discutetele con il resto della classe:

1. Pensate che potreste essere una vittima di alcuni dei crimini accennati durante la lezione?
2. Da una citazione di un membro di ISECOM: Per avere il background adeguato a valutare la prontezza della sicurezza di un sistema di elaborazione, o persino di un'intera organizzazione, è necessario possedere una comprensione fondamentale dei meccanismi di sicurezza e saper misurare il livello di assicurazione da disporre in quei meccanismi di sicurezza. Discutete qual'è il significato della citazione e come potreste prepararvi a valutare la prontezza della sicurezza di un sistema di elaborazione. Queste lezioni vi hanno fornito sufficienti materiali per cominciare?
3. [ esercitazione facoltativa per considerazione personale (discussione non generale) ]: Dopo avere analizzato le osservazioni in questa lezione, potete individuare attività tecnologiche di cui avete sentito parlare, o che avete fatto, che non avete mai

considerato come illegali, ma ora non siete sicuri. Una ricerca su Internet può contribuire a dissolvere i dubbi.

## 12.7. Approfondimenti consigliati

http://www.garanteprivacy.it

http://www.giustizia.it/cassazione/convegni/s15122000.htm

http://www.comellini.it/reatiinformatici.htm

http://www.parlamento.it/parlam/leggi/00248l.htm

http://www.interlex.it/testi/l41_633.htm

http://www.ftc.gov/bcp/menu-internet.htm

http://www.ic3.gov/

http://www.ccmostwanted.com/

http://www.scambusters.org/

http://compnetworking.about.com/od/networksecurityprivacy/l/aa071900a.htm

http://www.echelonwatch.org/

http://www.isecom.org/