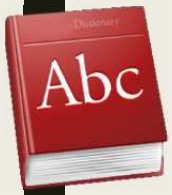
Outing And Trickery



Traduzione letterale: Outing: rivelazione, venire allo scoperto.
Trichery: frode, inganno.

- Comportamento che consiste nel pubblicare o condividere con terze persone le informazioni confidate dalla vittima in seguito a un periodo di amicizia in cui si è instaurato un rapporto di fiducia.
- L'aggressore pubblica su un Blog o diffonde attraverso e-mail o altre applicazioni, senza alcuna autorizzazione dell'interessato, le confidenze spontanee (outing) dell'amico e le sue fotografie riservate o intime. Oppure può sollecitare l'"amico" a condividere online dei segreti o informazioni imbarazzanti su se stesso, su un compagno di classe, su un amico comune o su un docente (trickery), per poi diffonderli ad altri utenti della rete

INFORMIAMOCI

Outing And Trickery

Si intende con il termine “outing” una forma di cyberbullismo attraverso la quale, il cyberbullo, dopo aver “salvato” (registrazione dati) le confidenze spontanee (outing) di un coetaneo (SMS, Chat, etc), o immagini riservate ed intime, decide, in un secondo momento, di pubblicarle su un Blog e/o diffonderle attraverso E-mail.
In altri casi, il cyberbullo può sollecitare, con l’inganno (trickery), “l’amico” a condividere online segreti o informazioni imbarazzanti su se stesso o un’altra persona per poi diffonderli ad altri utenti della rete, o minacciarlo di farlo qualora non si renda disponibile ad esaudire le sue richieste (talvolta anche sessuali).

Il cyberbullo può, dunque, avere inizialmente un rapporto bilanciato con la futura vittima, o quantomeno fingere di averlo, per poi assumere una posizione prevaricatoria – one up – e contare sul contributo attivo ma non necessariamente richiesto degli altri navigatori di internet.

L`Outing And Trickery non consiste nel pubblicare o condividere con terze persone le informazioni confidate dalla vittima in seguito a un periodo di amicizia in cui si è instaurato un rapporto di fiducia, ma può essere anche quando le persone hackerano il tuo account e iniziano a pubblicare foto, messaggi, conversazioni imbarazzanti e altro ancora sempre senza il tuo consenso.

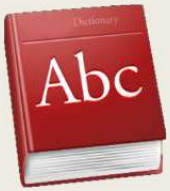
LA LEGGE DICE:

Outing and Trickery condotta criminale

- **art. 595 c.p.** comma III (diffamazione)
- **art. 615 bis c.p.** (interferenze illecite nella vita privata)
- **art. 528 c.p.** (pubblicazioni oscene) **depenalizzato dal d.lgs. n. 8/2016**

P

Pharming

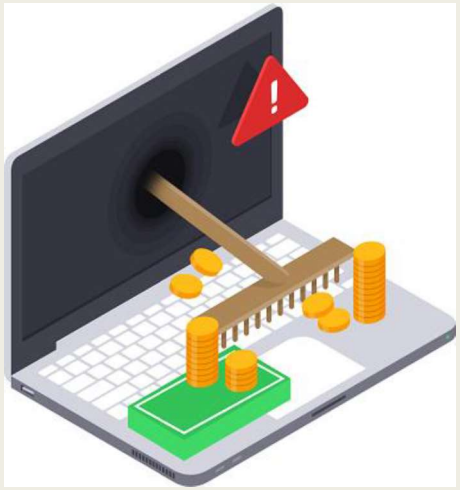


Traduzione letterale:
Composto dalle parole phishing (raggio telematico finalizzato all'acquisizioni di dati personali) e farming (coltivazione, allevamento).

- Forma di cybercrime che identifica un tentativo di phishing che può colpire più utenti simultaneamente

INFORMIAMOCI

Che cos'è il pharming?



Il pharming è una pratica fraudolenta simile al phishing. La differenza sta nel fatto che nel pharming il traffico legittimo di un sito web viene manipolato per reindirizzare gli utenti su siti fasulli che installeranno software dannosi sui computer dei visitatori o che preleveranno i dati personali degli utenti, come password o dati bancari. Il pharming è particolarmente insidioso in quanto, in caso di violazione di un server DNS, anche gli utenti con dispositivi pienamente protetti e privi di malware potranno esserne vittima.

Che tipi di pharming esistono?

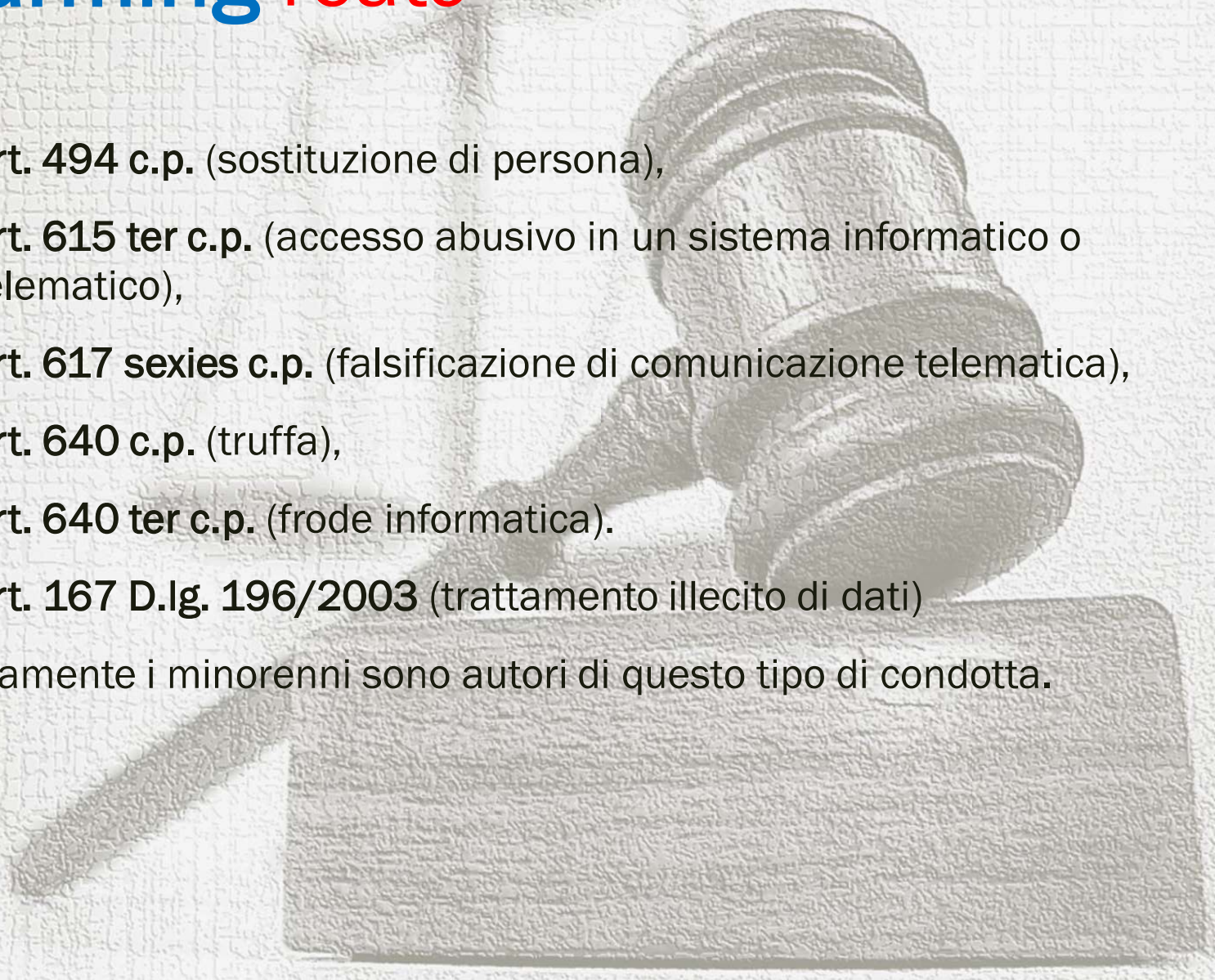
Il pharming assume due forme. Nella prima, gli hacker utilizzano svariati metodi per installare virus o altro malware sul computer delle ignare vittime. Il virus fa sì che il computer reindirizzi l'utente da un sito legittimo, come quello di una banca o di e-commerce, verso un sito fasullo progettato per avere lo stesso aspetto del sito che si desidera visitare. Il secondo tipo di pharming è quello che rende questo tipo di crimine informatico particolarmente pericoloso. In questa forma, un criminale informatico infetta un intero server DNS, reindirizzando ogni utente che cerca di visitare un sito legittimo verso quello fasullo.

Come si riconosce il pharming?

Se gli hacker fanno bene il loro lavoro, è quasi impossibile riconoscere un sito fasullo, creato per rubare dati, ma vi sono comunque alcuni aspetti da tenere d'occhio. Ad esempio, controllare sempre che l'URL del sito che si sta visitando sia scritto correttamente. Controllare sempre che l'URL venga modificato in “https”. La “s” sta per “secure” e indica che si tratta di un sito web sicuro.
(Avast.it)

LA LEGGE DICE:

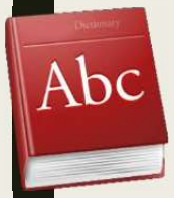
Pharming reato



- **art. 494 c.p.** (sostituzione di persona),
- **art. 615 ter c.p.** (accesso abusivo in un sistema informatico o telematico),
- **art. 617 sexies c.p.** (falsificazione di comunicazione telematica),
- **art. 640 c.p.** (truffa),
- **art. 640 ter c.p.** (frode informatica).
- **Art. 167 D.lg. 196/2003** (trattamento illecito di dati)

Rararamente i minorenni sono autori di questo tipo di condotta.

PHISHING



Trad. letterale: Raggio telematico finalizzato all'acquisizione di dati personali.

Questo tipo di truffa consiste nell'invio di e-mail fraudolente che invitano la vittima a collegarsi tramite un login a pagine internet (che imitano la grafica di siti istituzionali o aziendali) dalle quali verranno carpiti i loro dati riservati quali le credenziali per l'accesso a conti on-line, carte di credito, sistemi di pagamento tramite piattaforme e-commerce.

INFORMIAMOCI

PHISHING

Il phishing è una minaccia attuale, il rischio è ancora maggiore nei social media come *Facebook e Twitter.* Degli hacker potrebbero infatti creare un clone del sito e chiedere all'utente di inserire le sue informazioni personali. Gli hacker comunemente traggono vantaggio dal fatto che questi siti vengono utilizzati a casa, al lavoro e nei luoghi pubblici per ottenere le informazioni personali o aziendali. Secondo un'indagine realizzata nel 2019, solo il 17,93 per cento degli intervistati sarebbe in grado di identificare tutti i diversi tipi di phishing (tra cui email o sms contenenti link malevoli o siti web che replicano delle pagine legittime).

Lista dei tipi di phishing

Spear phishing

Clone phishing

Whaling

Manipolazione dei link

Aggiramento dei filtri

Contraffazione di un sito web

Phishing telefonico

(wikipedia.org/wiki/Phishing)

Istruzione

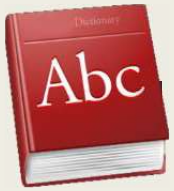
Una strategia per combattere il phishing è istruire le persone a riconoscere gli attacchi e ad affrontarli. L'educazione può essere molto efficace, specialmente se vengono enfatizzati alcuni concetti e fornito un feedback diretto.

LA LEGGE DICE:

PHISHING reato

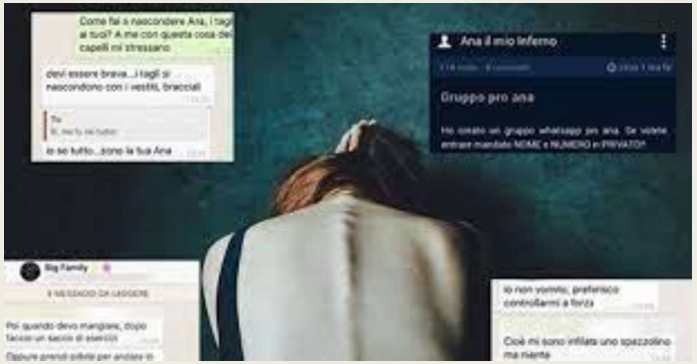
494 c.p. (sostituzione di persona)
art. 615 ter c.p. (accesso abusivo in un sistema informatico o telematico)
art. 617 sexies c.p. (falsificazione di comunicazione telematica)
art. 640 c.p. (truffa)
art. 640 ter c.p. (frode informatica).
art. 167 D.lg. 196/2003 (trattamento illecito di dati).

Pro Ana

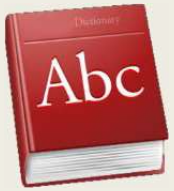


Traduzione letterale - Etimologia: composto da pro- e an(oressi)a.

- Termine che indica la promozione di comportamenti a favore dell'anoressia.
  In particolare siti, blog, community, etc, che esaltano l'anoressia e danno consigli per raggiungerla.



Pro Mia



Traduzione letterale - Etimologia: composto da pro- e (buli)mia.

Termine che indica la promozione di comportamenti a favore della bulimia.
In particolare siti, blog, community, etc, che esaltano la bulimia e danno consigli per raggiungerla.

INFORMIAMOCI

PRO ANA –PRO MIA

E’ attraverso i social che oggi, più che mai, si propaganda il canone estetico del corpo filiforme, con numeri ormai da pandemia sociale. Il luogo di ritrovo sono i blog “pro ana e pro mia”. E’ lì che le “amministratrici” reclutano ragazze, spesso poco più che bambine e le invitano a lasciare il loro numero di cellulare. Pochi minuti dopo si ritrovano inserite in un gruppi creati su watsapp per celebrare l’anoressia e la bulimia.

L’obiettivo minimo è perdere cinque chili in dieci giorni, ma con il passare del tempo diventa sempre più elevato. Nel gruppo compagne che insegnano a rifiutare il cibo e a vomitare, chi spiega che non puoi assumere più di dieci calorie al giorno, chi suggerisce di bere litri di acqua ghiacciata per ingannare la sensazione di fame, chi suggerisce di digiunare dopo le cinque del pomeriggio.

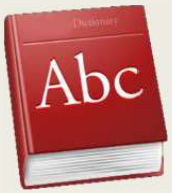
LA LEGGE DICE:

PRO ANA E PRO MIA comportamenti a rischio

- Condotte devianti che possono essere perseguibili dalla Procura minorile con la richiesta al Tribunale per i Minorenni di apertura di una procedura amministrativa ex artt. 25 "Misure applicabili ai minori irregolari per condotta o per carattere" - R.D.L. n. 1404 del 1934 (Articolo modificato con la Legge n. 888 del 1956) e/o di una procedura civile ex artt. 330 c.c. "Decadenza dalla responsabilità genitoriale sui figli" e 333 c.c. "Condotta del genitore pregiudizievole ai figli".

È stata recentemente avanzata una proposta di legge al Parlamento per sanzionare penalmente l'autore dei siti e/o blog pubblicati online.

PUP



Programma potenzialmente non desiderato

Trattasi di programma potenzialmente indesiderato che può essere involontariamente scaricato durante il download di un software. Si tratta quindi dell'inserimento, nel file d'installazione di un programma, di componenti superflui assolutamente non necessari per il funzionamento dell'applicazione alla quale si è interessati. Non si tratta quindi di un malware, creato con l'intento di danneggiare il computer o rubare informazioni personali, ma di un programma finalizzato a istallare senza consenso altri programmi indesiderati (ad esempio "adware" o "toolbar").

INFORMIAMOCI

PUP

Come operano i PUP?

In generale, si diffondono con l'installazione di software o componenti aggiuntivi del browser. Molte aziende responsabili dei PUP includono il download del programma indesiderato come operazione in background durante l'installazione, nella speranza che gli utenti non si accorgano della sua presenza. Una volta installati su un computer, possono essere utilizzati per consentire l'ingresso di altri tipi di malware sul sistema o per altre attività criminali.

Nel corso del 2015, Google ha effettuato ricerche che hanno rivelato come le reti PPI (pay per install), in cui i criminali informatici sono ricompensati per la massiccia distribuzione di adware, hanno colpito decine di milioni di utenti in tutto il mondo (5% delle IP). Secondo PandaLabs, nel secondo trimestre del 2014 c'è stata una rinascita dei PUP, che li ha visti rappresentare il 24,77% di tutte le infezioni da malware rilevate durante quel periodo.

Tipi di PUP

I PUP includono qualsiasi tipo di software che visualizza pubblicità intrusiva (adware)inietta il proprio contenuto pubblicitario sulle pagine Web visitate dall'utente o monitora le abitudini di Internet dell'utente per vendere informazioni agli inserzionisti (spyware)

E tutto ciò avviene attraverso un'installazione che viola il diritto al consenso informato. Alcune aziende li usano per dirottare i browser degli utenti (hijacking), cambiare la home page e il motore di ricerca predefinito. In questo modo, possono costringere l'utente ad accedere a Internet attraverso specifici siti Web, generando profitti per gli inserzionisti.

In alcuni casi, i criminali utilizzano il malware per rubare i cookie dei browser, dirottare le connessioni ai siti Web e agire sugli account degli utenti a loro insaputa o consenso (come l'installazione di app Android).

Alcuni pacchetti software indesiderati installano un certificato di root sui dispositivi degli utenti consentendo agli hacker di intercettare i dati riservati, come i dettagli bancari, e di bloccare gli avvisi di sicurezza.

Come evitarli

•Prima di installare un programma, gli esperti di sicurezza informatica raccomandano di scaricare sempre la versione più recente dal sito Web ufficiale del fornitore o da un sito di download affidabile.

•Controlla tutte le caselle di spunta durante l'installazione, dato che la maggior parte dei PUP utilizza tecniche di esclusione volontaria.

•Leggi l'informativa sulla privacy di tutti i programmi e le app che installi e verifica le autorizzazioni necessarie per installarli.

•Evita tutti i tipi di software sospetti, sia gratuiti che a pagamento.

•Utilizza un antivirus con rilevamento di malware e PUP

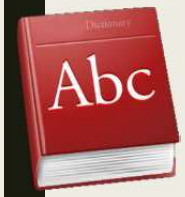
LA LEGGE DICE:

PUP condotta deviante

La condotta potrebbe diventare criminale nei casi in cui il sito di destinazione lucra sul traffico che è stato generato, **art. 640 c.p.** (truffa).

R

RICKROLLING



Trad. letterale: Rickrolling: distorsione, dannoso.

Trattasi di portare con l'inganno una persona a cliccare su un collegamento ipertestuale che porta invece a qualcosa di diverso da quanto sostenuto inizialmente. Un esempio celebre di Rickrolling è il caso della canzone "Never Gonna Give You Up" di Rick Astley a cui milioni di persone sono state reindirizzate cliccando link che fornivano informazioni su differenti aree tematiche.

INFORMIAMOCI

Funzionamento

Il fenomeno si basa su un meccanismo "ad esca": un utente di internet pubblica su un sito un collegamento web aggiungendo una descrizione particolarmente accattivante; il collegamento rimanda in realtà al video della canzone di Rick Astley, invece di rimandare a ciò che ci si aspettava di trovare. L'indirizzo web è generalmente mascherato in modo tale da non permettere di identificare l'URL di destinazione prima di cliccarvi sopra. Una persona che clicca sul collegamento e viene rimandata alla pagina web del video subisce un "rickroll". Il fenomeno si è esteso anche all'utilizzo del testo della canzone in luoghi inaspettati.

Origine

Si è sviluppato da un meccanismo simile chiamato "duckrolling", che era popolare sul sito web 4chan nel 2006. Il trucco del video ad esca è diventato popolare su 4chan dal giorno del pesce d'aprile 2007 e si è diffuso in altri siti web nello stesso anno.

Il primo rickrolling avrebbe avuto luogo il 5 Maggio 2007[, tramite un video pubblicato da un utente di YouTube.

Il fenomeno ha attirato l'attenzione del pubblico nel 2008 attraverso diversi eventi pubblicizzati, in particolare quando YouTube lo ha utilizzato nel suo evento Pesce d'aprile 2008.

LA LEGGE DICE:

RICKROLLING CONDOTTA DEVIANTE

La condotta diviene criminale nei casi in cui il sito di destinazione lucra sul traffico che è stato generato, **art. 640 c.p.** (truffa).

Raramente i minorenni sono autori di questo tipo di condotta.

Romance Scam

Traduzione letterale: Frode romantica.

Trattasi di una frode che prevede l'instaurazione di un contatto, attraverso chat, siti per single e piattaforme simili, con potenziali vittime che, illudendosi di avere iniziato una storia d'amore, sono disponibili a prestare o regalare importanti quantità di denaro.

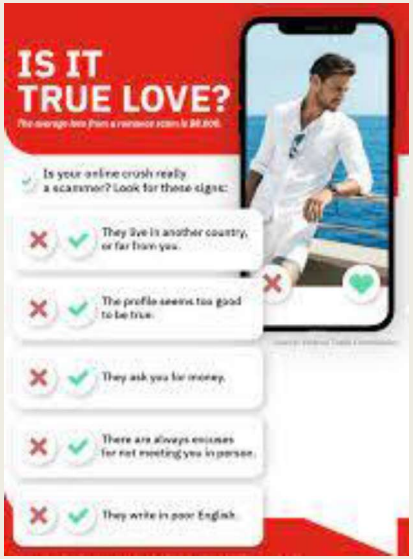
Vedi: **SCAM**

Romance Scam

Testimonianza anonima 18 dicembre 2012

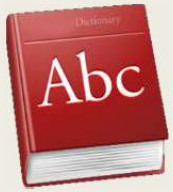
Ciao Amici sono stata anche vittima di un truffatore con identita' falsa. Mi ha contattato attraverso un sito di incontri. Ha detto che era vedovo che è venuto a Londra e aveva una galleria d'arte, e una figlia di nome Carla. Ha iniziato a mandarmi e-mail in amore ogni giorno. Ha detto che dopo aver vinto un contratto per l'acquisto di opere d'arte per la loro galleria in Malesia, sarebbe venuto in Brasile. Trascorsi pochi giorni dal suo arrivo in Malesia, mi scrisse di essere stato derubato in taxi e che, non potendo piu' comprare il biglietto aereo per il Brasile, mi chiedeva 1.500 dollari. Così gli ho mandato questo voucher con più 1.200 dollari per essere in grado di venire in Brasile.

Grazie alla ricerca che ho fatto su Internet ho scoperto questo sito dove anche altre donne sono state vittime.



S

SCAM



Trad. lett: Truffa, imbroglio, macchinazione.

Trattasi di modo illegale per ottenere denaro.
Questo genere di truffa può riguardare le seguenti aree:
1) trasferimento di importanti somme di denaro: in questo caso il truffatore chiede alla vittima un deposito cauzionale e/o il numero di conto corrente bancario e offre una ricompensa per il denaro recuperato;
2) vincita alla lotteria che può essere ritirata versando però una tassa;
3) messaggi sentimentali e successive richieste di aiuto economico per acquistare il biglietto aereo, curare una grave malattia o sostenere le spese burocratiche necessarie per acquisire i documenti per sposarsi;
4) richieste di matrimonio finalizzate ad ottenere la cittadinanza.

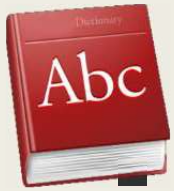
LA LEGGE DICE:

SCAM REATO

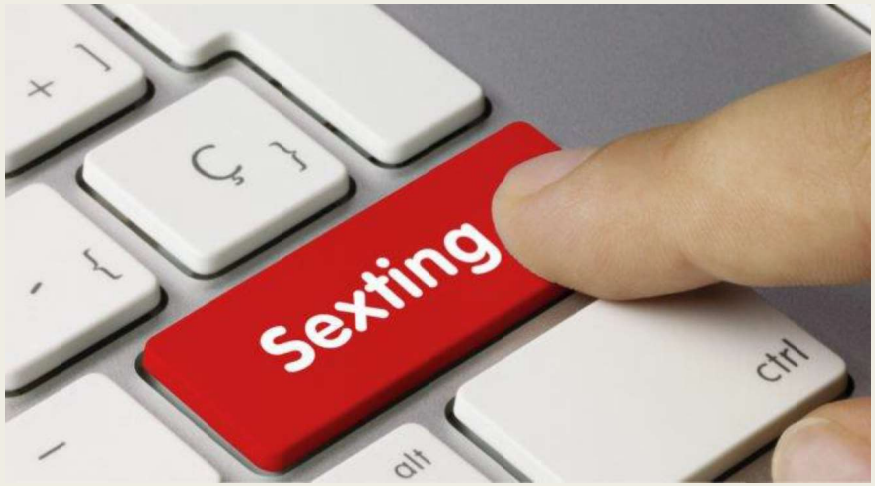
art. 640 c.p. (truffa)
art. 640 ter c.p. (frode informatica)
art. 494 c.p. (sostituzione di persona).

Sexting

- *Traduzione letterale*: Composto dalle parole sex (sesso) e texting (inviare SMS).



- Atto di inviare fotografie e/o messaggi di testo sessualmente espliciti. Solitamente tale comportamento viene posto in essere attraverso telefoni cellulare, ma anche tramite mezzi informatici differenti



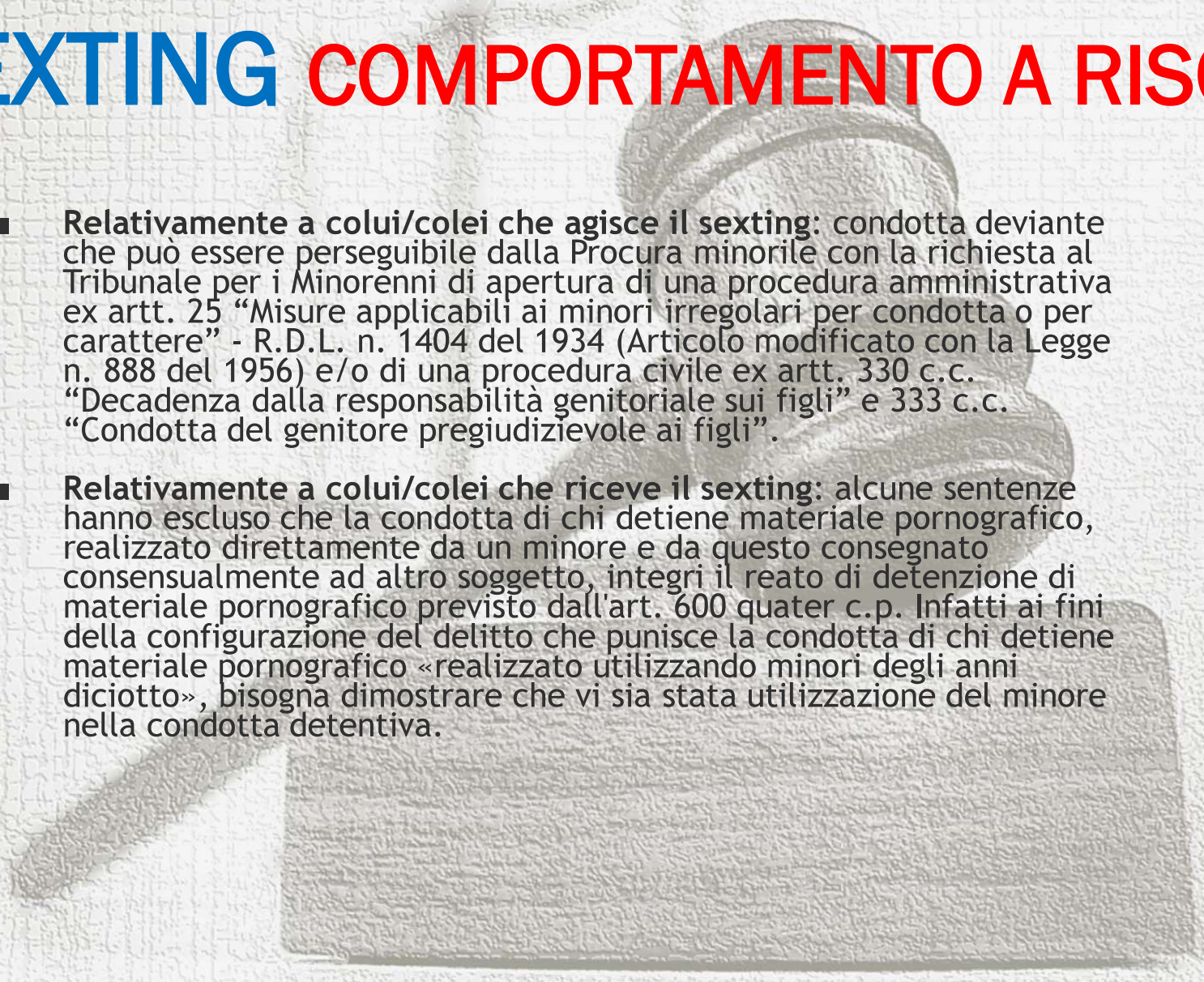
INFORMIAMOCI

Sexting

- **Rossellachiede aiuto**
- Alla linea 1.96.96 una mattina chiama Rossella, una ragazza di 15 anni, che piangendo riferisce di aver conosciuto in chat un ragazzo che adesso vuole ricattarla, mettendo un suo video su YouTube. Rossella racconta: «**Tutto è cominciato perché i miei amici mi avevano raccontato di una chat ed ero curiosa di capire come funzionasse**, e lì ho conosciuto un ragazzo che mi ha chiesto di conoscerci in una stanza privata. Una volta entrata lì, abbiamo iniziato a parlare attraverso una video chat, successivamente mi ha chiesto di spogliarmi e al mio rifiuto lui ha iniziato a ricattarmi dicendomi che mi avrebbe bloccato il pc. A quel punto, purtroppo, **ho ceduto al ricatto mi sono spogliata** e lui ha cominciato a farmi delle richieste, io o provato a dirgli che la mia mamma mi stava chiamando da un'altra stanza e che dovevo andare via ma lui mi ha detto di continuare altrimenti mi avrebbe bloccato tutto. Ad un certo punto, ho tentato, con una scusa ad allontanarmi e mi sono chiusa in bagno, adesso vi ho chiamato perché non so cosa fare, non so come comportarmi».
  L'operatrice tranquillizza la ragazza informandola che avendo contattato il **Telefono Azzurro** ha già fatto un passo importante per la propria sicurezza. Rossella, sentendosi rassicurata, fornisce gli elementi utili per risalire all'adescatore. Successivamente l'operatrice d'accordo con Rossella spiega alla madre della ragazza quanto accaduto e la invita a rivolgersi personalmente alle **Forze dell'Ordine** per sporgere formale denuncia. La madre si presenta con la ragazzina in Commissariato, sporge regolare denuncia nei confronti del presunto adescatore e viene informata la **Polizia Postale** e **la Procura presso il Tribunale dei Minori**.

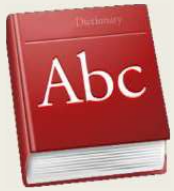
LA LEGGE DICE:

SEXTING COMPORTAMENTO A RISCHIO



- **Relativamente a colui/colei che agisce il sexting**: condotta deviante che può essere perseguibile dalla Procura minorile con la richiesta al Tribunale per i Minorenni di apertura di una procedura amministrativa ex artt. 25 “Misure applicabili ai minori irregolari per condotta o per carattere” - R.D.L. n. 1404 del 1934 (Articolo modificato con la Legge n. 888 del 1956) e/o di una procedura civile ex artt. 330 c.c. “Decadenza dalla responsabilità genitoriale sui figli” e 333 c.c. “Condotta del genitore pregiudizievole ai figli”.
- **Relativamente a colui/colei che riceve il sexting**: alcune sentenze hanno escluso che la condotta di chi detiene materiale pornografico, realizzato direttamente da un minore e da questo consegnato consensualmente ad altro soggetto, integri il reato di detenzione di materiale pornografico previsto dall'art. 600 quater c.p. Infatti ai fini della configurazione del delitto che punisce la condotta di chi detiene materiale pornografico «realizzato utilizzando minori degli anni diciotto», bisogna dimostrare che vi sia stata utilizzazione del minore nella condotta detentiva.

Sextortion Scams



Traduzione letterale: Deriva dall'unione delle parole inglesi "sex" (sesso) ed "extortion" (estorsione).

- Trattasi di truffa perpetrata ai danni di utenti internet ai quali, con l'illusione di un flirt o una storia sentimentale, sono estorte immagini erotiche usate poi come strumento di ricatto.

INFORMIAMOCI

Sextortion Scams

Il 22 giugno 2021, l'RCMP del distretto di Halifax ha ricevuto un rapporto di sextortion in cui la vittima ha avuto una chat video con il sospetto. Secondo la polizia, il sospettato ha registrato la chiamata e ha inviato uno screenshot alla vittima chiedendo soldi. La polizia dice che non è stato inviato denaro. La vittima in questo caso era un ragazzo di 18 anni.

Il termine sextortion è stato utilizzato per descrivere una situazione in cui una relazione online evolve al punto in cui il sospettato, che la vittima ha incontrato solo online, chiede alla vittima di compiere un atto sessuale durante una video chat online. Il sospettato rivela quindi alla vittima di aver registrato l'atto, chiede denaro e minaccia di rilasciare il video ai contatti della vittima se non si conformano.

La polizia dice che mentre i video non sono stati inviati ai contatti della vittima in questo caso particolare, come il sospetto ha minacciato di fare, ciò non significa che non accadrà mai.

"Se fai un video o scatti una foto e quel dispositivo ha la capacità di connettersi a Internet, il contenuto può essere visto da chiunque", afferma S/Sgt. Royce MacRae, di Nova Scotia RCMP Digital Forensics Services. "Un modo per proteggersi da questo tipo di truffa è non accettare richieste di amicizia da estranei ed evitare di condividere contenuti intimi online con persone che non hai mai incontrato di persona".

L'indagine è in corso.

https://atlantic.ctvnews.ca/n-s-rcmp-warn-public-about-sextortion-scams

LA LEGGE DICE:

Sextortion Scams REATO

- **art. 629 c.p.** (estorsione)
- **art. 595 c.p. comma III** (diffamazione)
- **art. 615 bis c.p.** (interferenze illecite nella vita privata)
- **art. 528 c.p.** (pubblicazioni oscene) **depenalizzato dal d.lgs. n. 8/2016**
- **art. 610 c.p.** (violenza privata)

-**art. 612 c.p.** (minacce).

SMISHING AND VISHING

Trad. lett: Truffa con sms (da SMS + phishing).
Trattasi di truffa riconducibile al phishing, effettuata attraverso gli SMS. La vittima riceve SMS da un falso mittente che ha il fine ultimo di ottenere in modo fraudolento i suoi dati d'accesso ai servizi online (banca, carta di credito, etc).

Trad. lett: Truffa a mezzo voce (da Voice + phishing).
Trattasi di truffa riconducibile al phishing, perpetuata attraverso una chiamata telefonica.

SMISHING AND VISHING

L'azione di questi **pirati informatici** è sempre più sofisticata, poi, visto che l'introduzione dell'autenticazione forte nel **2018**, come conseguenza della ***PSD2*** e dei relativi regolamenti ***EBA***, ha reso molto più difficile poter effettuare delle frodi partendo dai profili di home-banking ed è necessaria un'azione diretta della vittima per poter violare i sistemi di sicurezza. Tutto parte, quindi, con il messaggio allarmante e l'esortazione ad accedere al proprio profilo partendo da un **link** indicato nel testo. Se lo si cliccasse, questo condurrebbe direttamente a un **sito clone** ma della pagina di login della banca della vittima: la maschera mostrata è, poi, pensata appositamente per ottenere le informazioni che si volessero. Solitamente i campi da compilare sono il codice cliente, la password e un altro, che non è mai presente nei siti originali, con la richiesta di inserimento del numero di cellulare. Se l'autenticazione forte fosse prevista via SMS, allora, dopo poco partirebbe quello che viene chiamato ***SIM swap***, cioè la clonazione della scheda SIM per permettere ai pirati di accedere e autenticare le operazioni mentre il telefono della vittima smetterebbe di funzionare, impedendogli di bloccare immediatamente il profilo o di avvisare per tempo la propria banca.

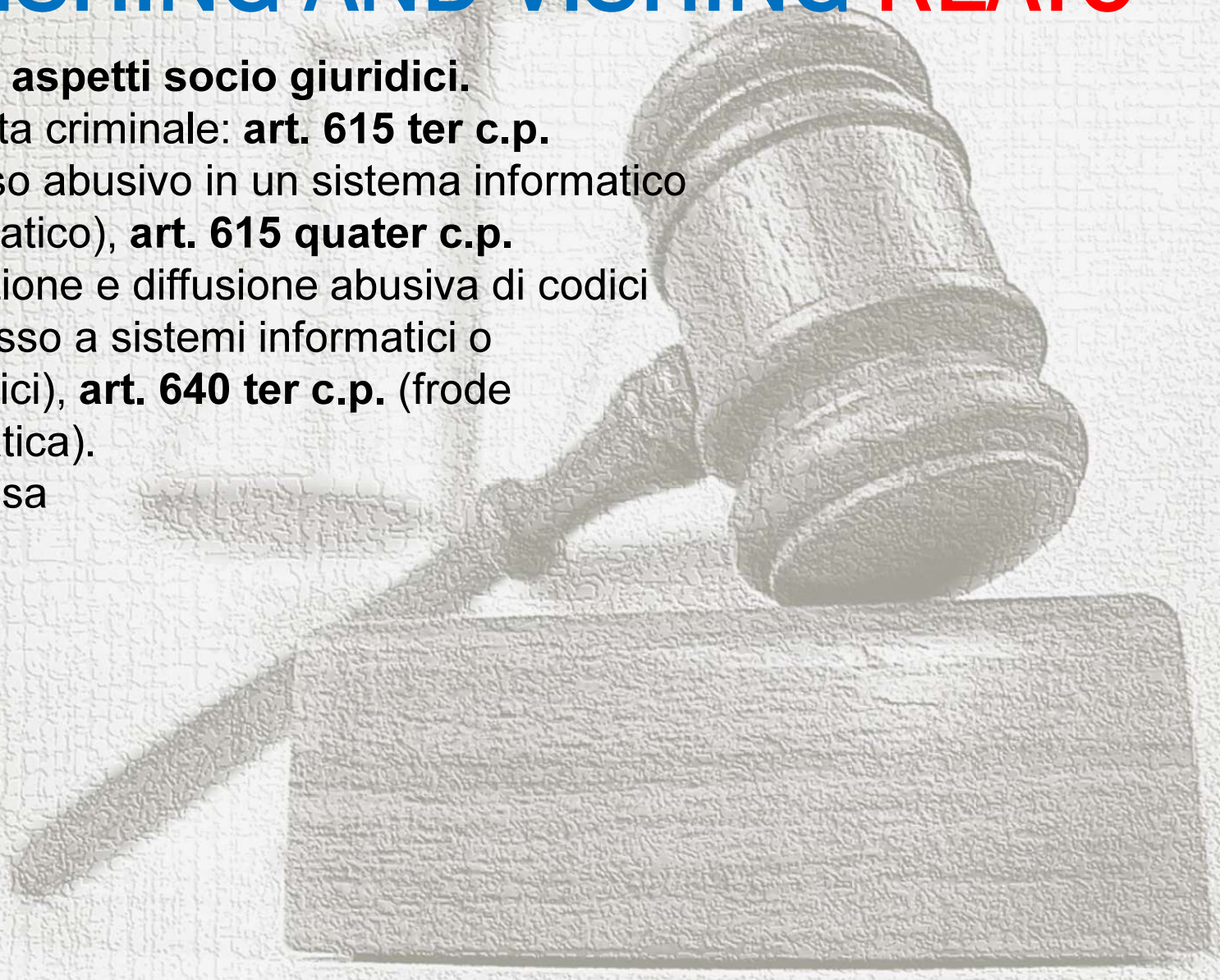
Dal lato dell'home banking occorre sempre ricordare che i codici di accesso siano **personali** e **non cedibili** a nessuno, in primis, e che in caso di ricezione di messaggi sospetti non bisogna **mai rispondere** né seguire le istruzioni indicate ma segnalarli alla propria banca, in secundis.

https://www.interris.it/rubriche/opinione/phishing-smishing/

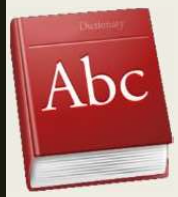
LA LEGGE DICE:

SMISHING AND VISHING REATO

Sintesi aspetti socio giuridici.
Condotta criminale: **art. 615 ter c.p.** (accesso abusivo in un sistema informatico o telematico), **art. 615 quater c.p.** (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici), **art. 640 ter c.p.** (frode informatica).
Si precisa



SNIFFING



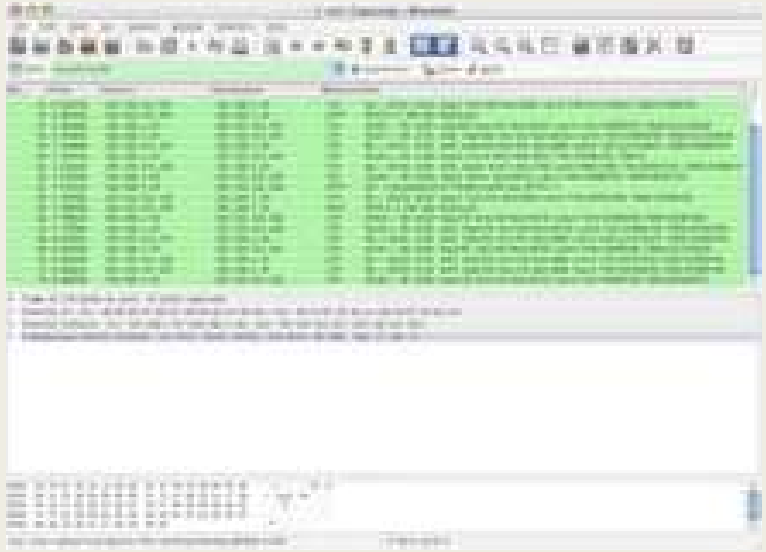
Trad. lett: Sniffare, annusare, fiutare.

Definisce l'attività di intercettazione dei dati che transitano in una rete telematica. Tale attività può avere finalità legittime (risolvere problemi tecnici o evitare intrusioni da parte di terzi) oppure illecite (ottenere password, codici per l'home banking, dati sensibili, ecc).

INFORMIAMOCI

SNIFFING

I prodotti software utilizzati per eseguire queste attività vengono detti sniffer ed oltre ad intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso: questi intercettano i singoli pacchetti, decodificando le varie intestazioni di livello datalink, rete, trasporto, applicativo, potendo offrire inoltre strumenti di analisi che analizzano ad es. tutti i pacchetti di una connessione TCP per valutare il comportamento del protocollo di rete o per ricostruire lo scambio di dati tra le applicazioni.



Lo sniffing pone problemi di privacy in quanto accede senza mandato e a insaputa dell'utente ad un computer che è sua proprietà privata nonché ad una rete che è proprietà di chi diffonde il software di accesso. In generale, l'accesso ad un'abitazione o altra proprietà privata per una perquisizione richiede un mandato della magistratura e che esso sia mostrato al proprietario del bene perquisito.

I dati forniti dall'Internet Service Provider non identificano la persona, ma l'utenza telefonica. Non necessariamente poi la persona che ha commesso il fatto è un componente del nucleo familiare, al quale è intestata l'utenza. Tramite un WISP o una rete wireless domestica è più facile che si verifichino violazioni della rete e accessi abusivi dall'esterno. La non-identificazione di chi commette materialmente il fatto esclude un nesso di causalità fra la connessione alla rete P2P e la violazione del diritto d'autore, e non è una prova sufficiente per gli effetti penali previsti dalla legge. Per l'ambito penale, serve un accertamento univoco e inequivocabile della persona e delle responsabilità. Tuttavia, il titolare della utenza telefonica può essere ritenuto responsabile della sua sicurezza e del suo utilizzo, e rispondere dell'illecito amministrativo.

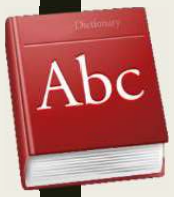
wikipedia.org/wiki/Sniffing

LA LEGGE DICE:

SNIFFING condotta criminale

art. 615 ter c.p. (accesso abusivo in un sistema informatico o telematico),
art. 615 quater c.p. (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici),
art. 640 ter c.p. (frode informatica).

Spamming



Traduzione letterale: Inondazione (di caselle di altri utenti) con messaggi indesiderati.

- Trattasi dell'invio di mail indesiderate (generalmente di tipo commerciale/pubblicitario) a un gran numero di destinatari che non hanno prestato il proprio consenso ("opt in") a questa ricezione, creando di conseguenza l'intasamento della casella di posta elettronica.
- Talvolta può essere utilizzato anche il termine **Junk-Mail**

Spamming

Al giorno d'oggi siamo piuttosto abituati a combattere contro lo **spamming**, tant'è che ormai lo consideriamo una sorta di "male" che è necessario sopportare quando si decide di aprire una casella di posta elettronica. I provider cercano di combatterlo come possono, spesso attraverso filtri anti spam, ma qualche mail di spamming riesce sempre a sfuggire da questo meccanismo.

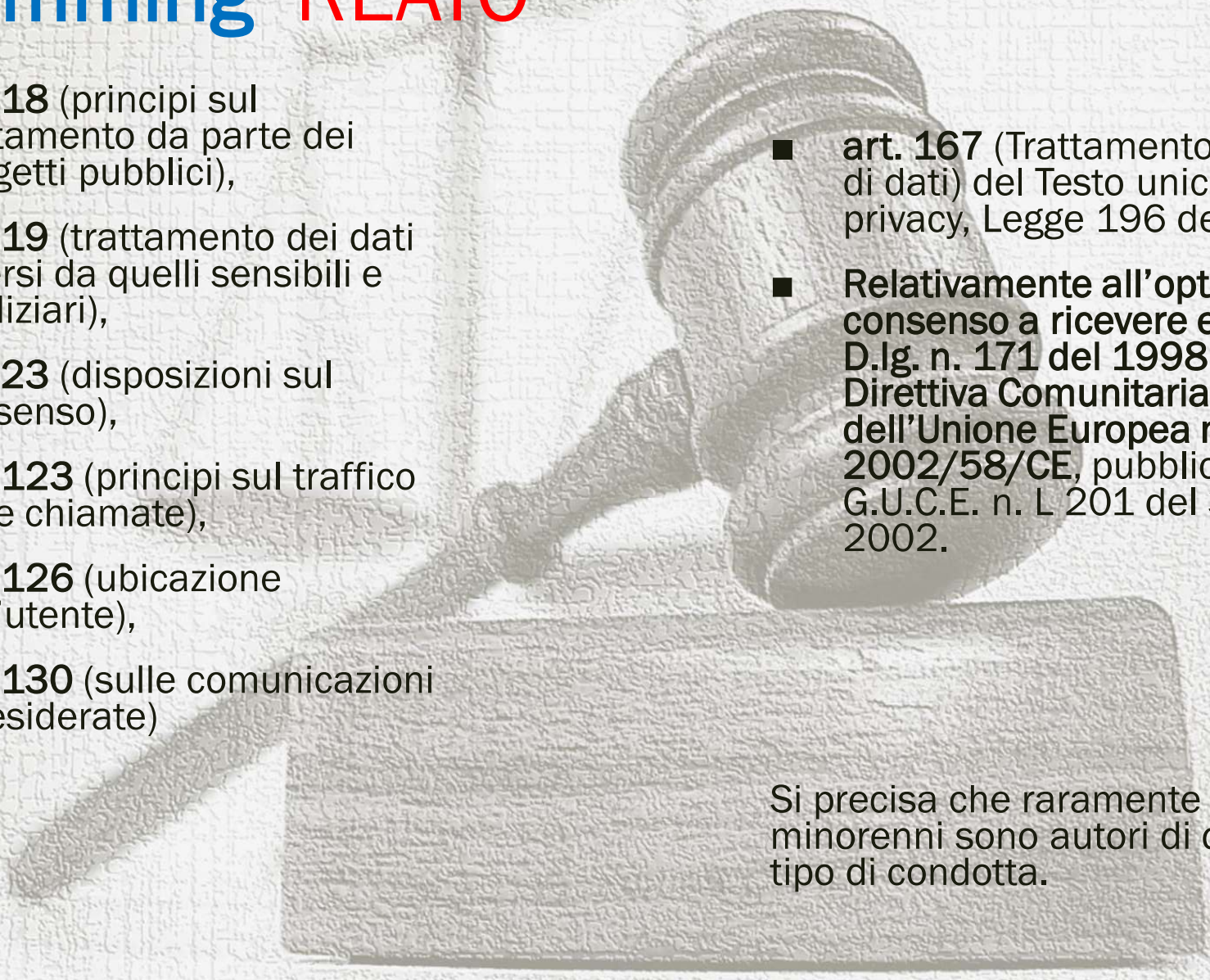
Tanto più che moltissimi messaggi giungono alla nostra casella di posta perché sottoscriviamo – spesso inconsapevolmente – servizi che cedono il nostro indirizzo di posta elettronica ad aziende terze, che poi iniziano ad inviare newsletter sui propri servizi.

Il termine spam, però, venne coniato soltanto nel 1993, da Richard Depew, moderatore di un newsgroup che l'aveva sentito in uno sketch dei Monty Python, in riferimento al noto marchio di carne Spam.

LA LEGGE DICE:

Spamming REATO

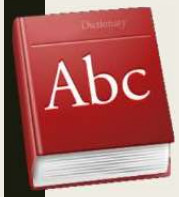
- **art. 18** (principi sul trattamento da parte dei soggetti pubblici),
- **art. 19** (trattamento dei dati diversi da quelli sensibili e giudiziari),
- **art. 23** (disposizioni sul consenso),
- **art. 123** (principi sul traffico delle chiamate),
- **art. 126** (ubicazione dell'utente),
- **art. 130** (sulle comunicazioni indesiderate)



- **art. 167** (Trattamento illecito di dati) del Testo unico sulla privacy, Legge 196 del 2003.
- **Relativamente all'opt in (il consenso a ricevere email): D.lg. n. 171 del 1998, Direttiva Comunitaria dell'Unione Europea n. 2002/58/CE**, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002.

Si precisa che raramente i minorenni sono autori di questo tipo di condotta.

SPEARPHISHING



Trad. Let: Spear: lancia, arpione + phishing.

Trattasi di campagne di truffe mirate. Dopo avere osservato online gli interessi delle vittime (grazie alle informazioni che pubblicano nei social network), i truffatori inviano email non più generiche, come nel phishing classico, ma personalizzate, rendendo con i dettagli in esse contenute più credibile il messaggio.

Il phishing si sta evolvendo costantemente, prendendo sembianze di volta in volta diverse, come quella dello **spear-phishing** che mette nel mirino utenti specifici.

INFORMIAMOCI

SPEARPHISHING

Come difendersi?

Sistema di filtraggio delle comunicazioni via e-mail

Al giorno d'oggi, all'interno di un contesto aziendale e organizzativo è fondamentale utilizzare un sistema di filtraggio delle e-mail.
Sono disponibili soluzioni "on-premises" e su cloud in grado di riconoscere pattern d'attacco e proteggere i destinatari in modo automatizzato (non facendo arrivare il messaggio) o notificando i rischi collegati all'apertura di allegati e link.

A livello generale, **tutti gli elementi software e hardware andrebbero aggiornati costantemente** per evitare che vulnerabilità note offrano l'apertura a violazioni, data breach o altri problemi. Il tempo che intercorre fra il rilascio delle patch e l'installazione dovrebbe essere ridotto al minimo e tale approccio dovrebbe essere condiviso a livello aziendale.

Attenzione alle piattaforme per la condivisione di file

Lo smart working ha reso necessario l'utilizzo di programmi per la condivisione e la comunicazione a distanza. Per garantire standard di sicurezza alti, è opportuno porre una stretta rispetto a tale pratica, o perlomeno fornire delle linee guida chiare sulle piattaforme di condivisione considerate sicure dal management societario. Va poi ricordato che permane il rischio di "spoofing" ovvero di piattaforme che imitano quelle legittime per inviare messaggi, link o richieste specifiche di compiere una determinata azione.

L'importanza del fattore umano

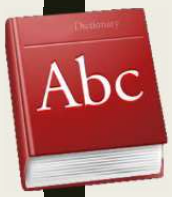
Parlando di phishing e spear-phishing è bene ricordare la centralità del fattore umano.
Sicuramente gli strumenti e gli approcci automatici e tecnologici che abbiamo visto finora sono utili a "scremare" e ridurre i rischi. Ma nel caso in cui un'offensiva riesca a penetrare le prime mura difensive, è opportuno che ad accoglierla ci sia una risorsa umana preparata.

https://www.giornalettismo.com/spear-phishing-come-difendersi/

LA LEGGE DICE:

SPEARPHISHING condotta criminale

art. 494 c.p. (sostituzione di persona),
art. 615 ter c.p. (accesso abusivo in un sistema informatico o telematico),
art. 617 sexies c.p. (falsificazione di comunicazione telematica),
art. 640 c.p. (truffa), **art. 640 ter c.p.** (frode informatica).



SPIM

Trad. let: Acronimo di Messaging Spam.

Nelle applicazioni di Instant Messaging, indica lo spamming che generalmente, invita l'utente a collegarsi a un sito web.

INFORMIAMOCI

SPIM

Sono noti come spim tutti quei messaggi che ti arrivano attraverso varie chat, messaggi istantanei e SMS, che non hai richiesto e contengono informazioni che non sono rilevanti per te.

Si potrebbe dire che si tratta di un tipo di frode utilizzato da alcuni programmi che agiscono automaticamente. In questo modo riescono a raggiungere gli utenti e inviare loro messaggi pubblicitari nelle diverse applicazioni di messaggistica che utilizzano.

Una volta che questi programmi automatici hanno “rubato” l’elenco dei contatti di una società, inizieranno a inviare messaggi agli utenti. Questi testi a volte includono collegamenti che indirizzano a download automatici di malware o a siti fraudolenti. Anche se sono pratiche comuni, molti si chiedono come funzionino esattamente.

Nella peggiore delle sue versioni, lo spim è una frode online che viene eseguita tramite applicazioni automatizzate, che otterranno le informazioni di contatto che hanno le applicazioni di messaggistica istantanea. Questi messaggi appariranno attraverso finestre pop-up nelle tue conversazioni.

Ecco perché spim e spam hanno una grande somiglianza, poiché entrambi ti fanno correre gli stessi rischi. La differenza è che usano media diversi.

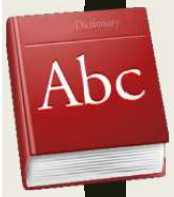
https://www.mdirector.com/

LA LEGGE DICE:

SPIM condotta criminale

art. 18 (principi sul trattamento da parte dei soggetti pubblici),
art. 19 (trattamento dei dati diversi da quelli sensibili e giudiziari),
art. 23 (disposizioni sul consenso),
art. 123 (principi sul traffico delle chiamate),
art. 126 (ubicazione dell'utente),
art. 130 (sulle comunicazioni indesiderate) e **art. 167** (Trattamento illecito di dati) del Testo unico sulla privacy,
Legge 196 del 2003.
Relativamente all'*opt in* (il consenso a ricevere email): D.lg. n. 171 del 1998,
Direttiva Comunitaria dell'Unione Europea n. 2002/58/CE, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002.

SPOOFING



Trad. lett: Presa in giro; farsi beffa di qualcuno.

Trattasi di comportamento messo in atto dallo spoofer.
Spoofer è colui che falsifica dati e protocolli con l'intento di apparire un'altra persona o di accedere ad aree riservate.
Le tecniche di spoofing sono diverse, le più note e adoperate sono32:
- Spoofing dell'IP (falsificazione di pacchetti IP al fine di nasconderne la presenza) 33
- Spoofing del DSN
- Spoofing dell'ARP
- Web Spoofing
- SMS Spoofing
- Mail Spoofing

INFORMIAMOCI

SPOOFING

Lo spoofing è ciò che fa un cybercriminale quando finge di essere una fonte affidabile per ottenere accesso a informazioni importanti. Di solito, l'obiettivo principale dello spoofing è accedere a dati personali, rubare denaro, bypassare i controlli di accesso alle reti o diffondere malware tramite link e allegati infetti.
Coinvolge pratiche differenti e nella maggior parte dei casi fa leva sui punti deboli del carattere umano, ad esempio sulla paura (vedi le truffe legate al coronavirus), sull'ingenuità della vittima o sulla sua avidità. Di conseguenza, i truffatori cercano sempre nuove categorie di persone vulnerabili tramite procedimenti che possono sfruttare più livelli informatici: sito web, e-mail, telefonata, SMS, indirizzo IP e server.
Alcuni degli spoofing più comuni hanno degli elementi o indizi che devono mettere l'utente in guardia. Se si sospetta invece di aver già subito un attacco, alcuni dei seguenti **elementi aiutano a identificarne la tipologia.**

Spoofing E-mail Controllare gli indirizzi dei mittenti – I truffatori creano indirizzi simili a quelli dei contatti della vittima per ingannarla. Se l'e-mail ha un contenuto sospetto ma l'indirizzo sembra esatto, è consigliato contattare il mittente per chiedere conferma.

Messaggi con errori – In caso di un messaggio contenente errori grammaticali o ortografici, è possibile che si tratti di un tentativo di phishing. Fare delle ricerche online è il metodo migliore per verificare l'autenticità del messaggio. Cercare info sul mittente o contattarlo oppure copiare il corpo dell'e-mail e incollarlo nella casella di ricerca di Google, inserendolo tra virgolette. In caso di risultati significa che il messaggio è preconfezionato e si tratta di una truffa.

Spoofing del sito web Controllare la barra degli indirizzi - Normalmente gli hacker non acquistano certificati SSL per i domini dei propri siti di phishing. Per questo motivo, in caso di dubbi la prima cosa da fare è controllare la barra degli indirizzi del browser e vedere se il protocollo della pagina è HTTPS o solo HTTP, senza la S finale. La S del protocollo https sta per sicuro e significa che il sito è crittografato e protetto dai cybercriminali.

Utilizzare un password manager, software che compilano automaticamente i moduli di login non funzionano sui siti oggetto di spoofing. Se il tuo password manager non dovesse funzionare automaticamente sarebbe il caso di insospettirsi.

Non trovare l'icona del lucchetto – Un ulteriore indizio grafico della sicurezza di un sito web è la piccola icona a forma di lucchetto o una barra verde chiaro a sinistra dell'URL.

Spoofing dell'ID chiamante- Ricevere chiamate da numeri sconosciuti - Quasi sicuramente si tratta di spam oppure il numero di telefono è oggetto di spoofing. Non rispondere mai a queste chiamate, soprattutto se la chiamata proviene dall'estero

Ricevere risposte a domande mai poste - Incongruenze di questo tipo sono sempre sintomi di minacce informatiche. Ad esempio, ricevere un SMS o un'e-mail il cui oggetto inizia con "RE:" (risposta) e fa riferimento ad una conversazione precedente.

Panda Security ha elaborato dei consigli per difendersi dalle diverse tipologie di spoofing:

•**Attivare il filtro dello spam**: in questo modo, la maggior parte delle e-mail di spoofing verranno bloccate prima di raggiungere la tua casella di posta.

•**Esaminare la comunicazione**: come anticipato, i messaggi utilizzati negli attacchi di spoofing spesso contengono errori grammaticali, di formato o semplicemente affermazioni poco credibili

•**Verificare le informazioni**: se una mail o una chiamata sono sospette, fare un passaggio di verifica con il mittente per confermare la veridicità delle informazioni contenute nel messaggio.

•**Individuare nome/destinazione completa**: se un URL o un allegato di una mail non ti convince, passaci sopra il mouse per visualizzare la destinazione esatta o il nome completo del file.

•**Impostare l'autenticazione a due fattori**: è il metodo più sicuro in assoluto per proteggere i tuoi account digitali. Per contenuti altamente sensibili si potrebbe ricorrere ad un token di sicurezza, aggiungendo così un livello hardware al sistema di protezione informatica.

•**Investire in un software professionale di cybersecurity:** a livello di dispositivo è indispensabile installare un programma di sicurezza informatica efficace.

Lo spoofing continua ad essere molto efficace ed è per questo regolarmente impiegato nei cyberattacchi (spear phishing) a causa dell'incuranza e della poca formazione degli utenti. Se si ritiene di essere vittima di un attacco di spoofing, bisogna segnalarlo immediatamente alla Polizia Postale e al proprio provider di servizi internet, così potranno indagare più a fondo e fermare il cybercriminale prima che faccia altre vittime. Inoltre, se a causa di un attacco di spoofing si è perso denaro, la denuncia di furto deve essere immediata.

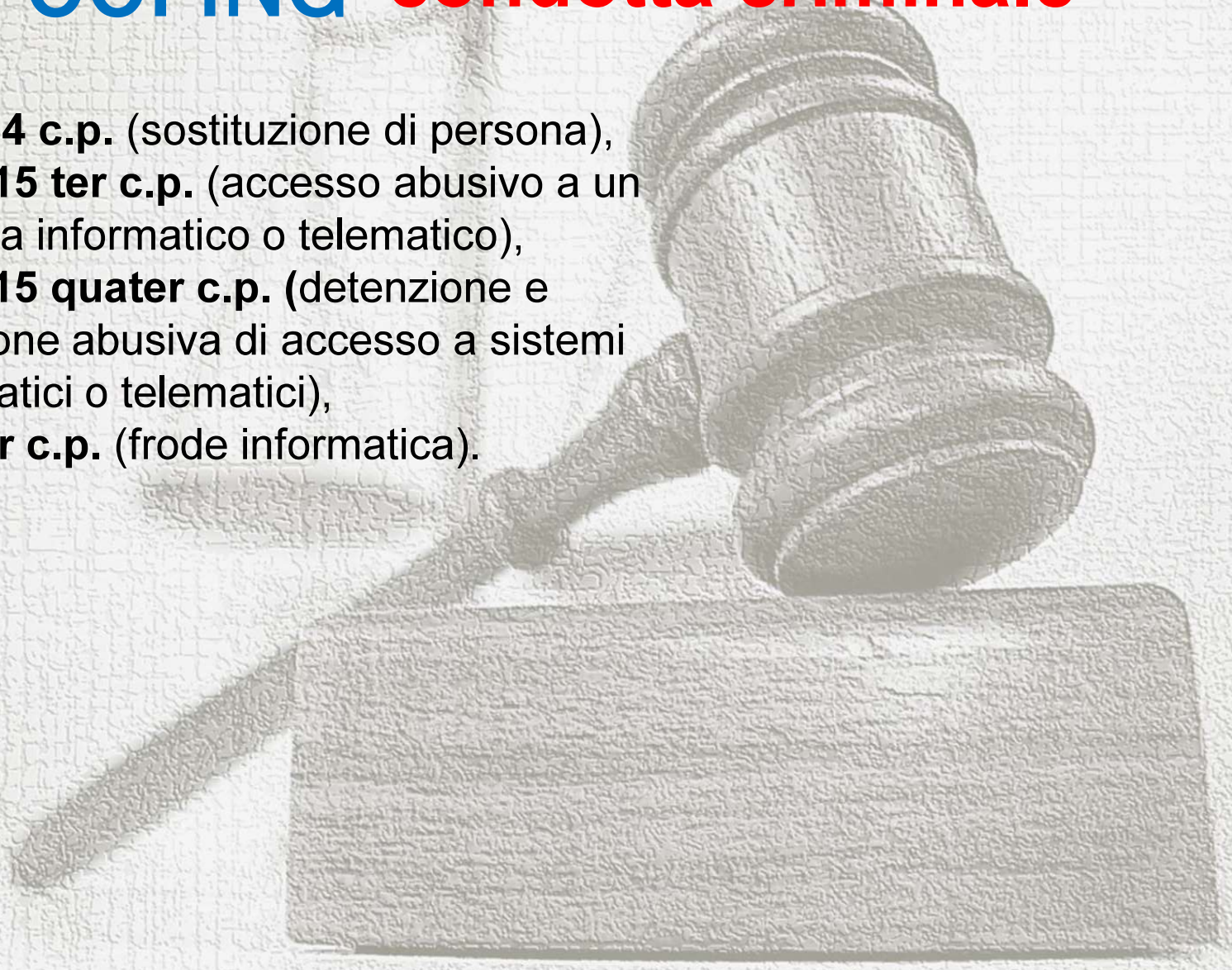
Purtroppo, le minacce digitali sono varie ed in continua evoluzione, per questo è necessario migliorare sempre di più il proprio sistema di sicurezza informatico.

https://www.informazione.it/

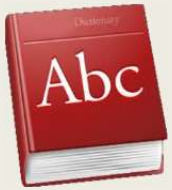
LA LEGGE DICE:

SPOOFING condotta criminale

art. 494 c.p. (sostituzione di persona),
art. 615 ter c.p. (accesso abusivo a un sistema informatico o telematico),
art. 615 quater c.p. (detenzione e diffusione abusiva di accesso a sistemi informatici o telematici),
640 ter c.p. (frode informatica).



STREAPNOMINATION



Trad. Let: Nomination dello streep tease

Si indica il comportamento di una persona che, nominata da un amico online, si spoglia in un luogo pubblico e affollato al fine di produrre un video che sarà poi diffuso nei principali social network.

LA LEGGE DICE:

STREAPNOMINATION condotta criminale

art. 527 c.p. (atti osceni),
art. 528 c.p. (pubblicazioni oscene).