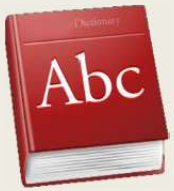
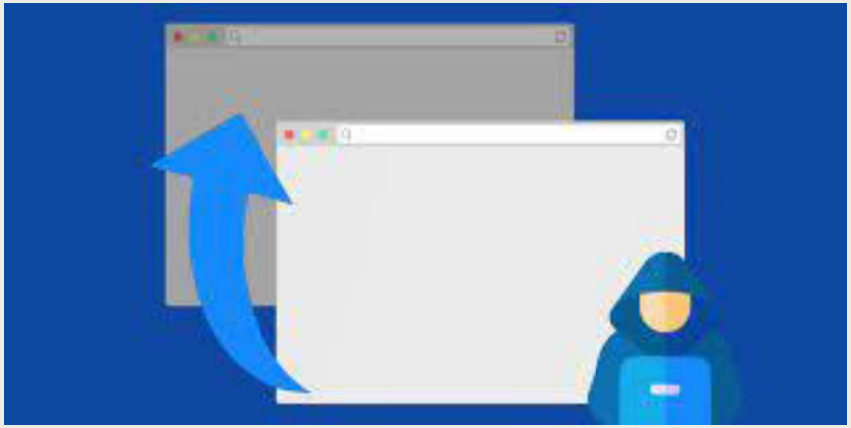
T

TABNABBING



Trad. lett: Catturare la scheda di un browser.

Trattasi di truffa online che prende di mira le schede aperte (TAB) nel browser sostituendone il contenuto con una pagina identica, creata appositamente per richiedere all'utente a inserire i propri dati personali che saranno poi copiati. È una forma più raffinata di phishing.

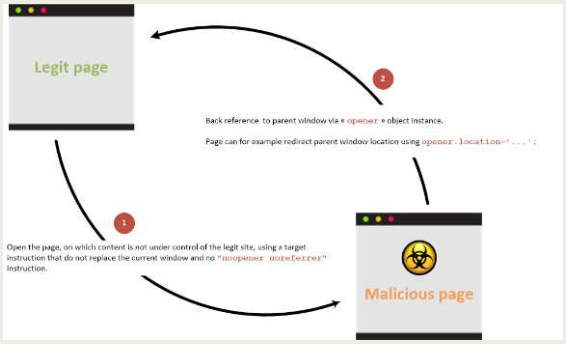


TABNABBING

L'attacco sfrutta la fiducia degli utenti e la disattenzione per i dettagli relativi alle schede e la capacità dei browser di navigare attraverso l'origine di una pagina nelle schede inattive molto tempo dopo il caricamento della pagina. Il tabnabbing è diverso dalla maggior parte degli attacchi di phishing in quanto l'utente non ricorda più che una determinata scheda era il risultato di un collegamento non correlato alla pagina di accesso, perché la pagina di accesso falsa viene caricata in una delle schede aperte di lunga durata nel proprio browser.

L'attacco fa sì che il browser acceda alla pagina rappresentata dopo che la pagina è stata lasciata incustodita per un po' di tempo. Un utente che ritorna dopo un po' e vede la pagina di login può essere indotto a credere che la pagina sia legittima e ad inserire il proprio login, password e altri dettagli che verranno utilizzati per scopi impropri.

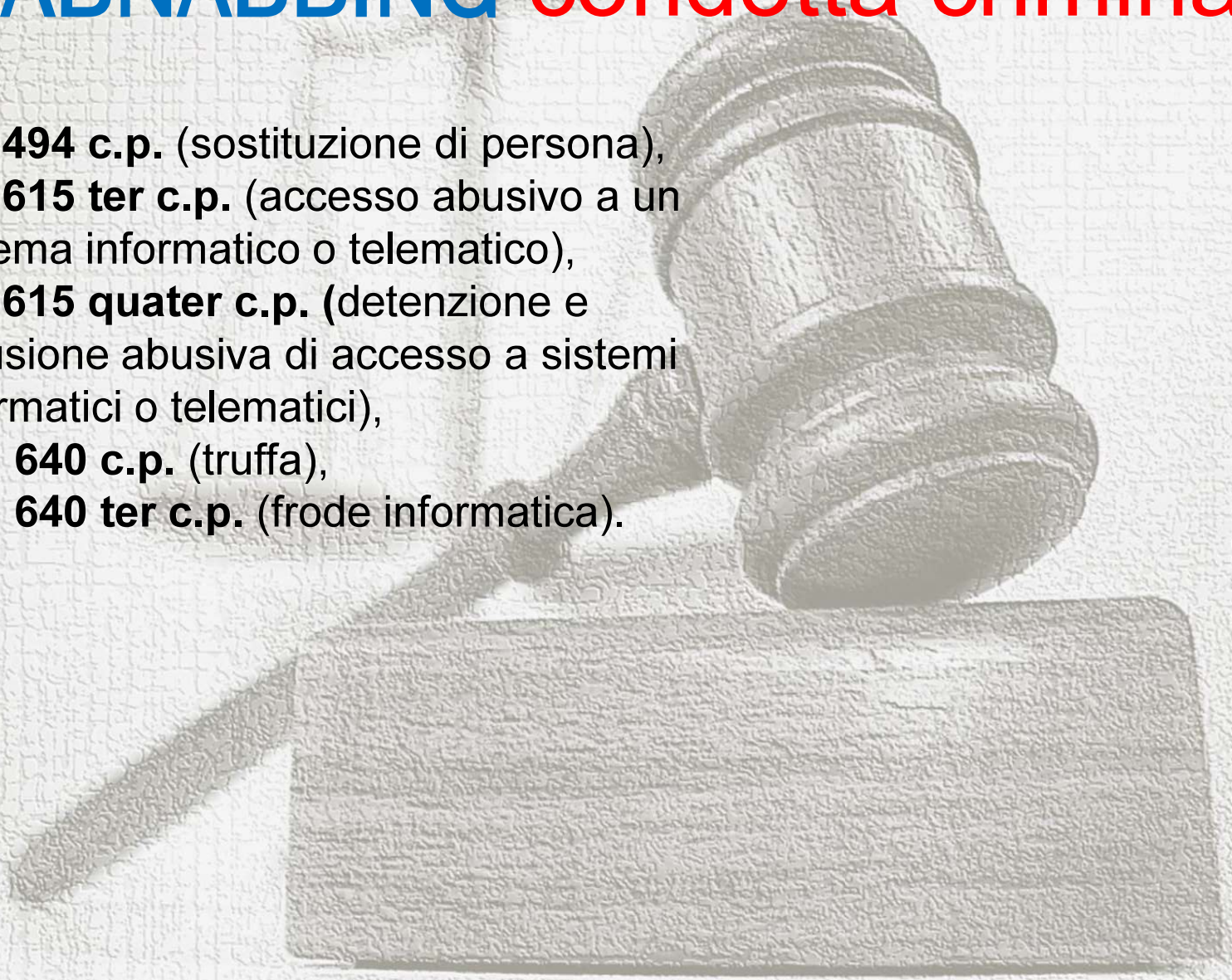
https://en.wikipedia.org/wiki/Tabnabbing



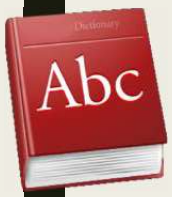
LA LEGGE DICE:

TABNABBING 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),
art. 640 c.p. (truffa),
art. 640 ter c.p. (frode informatica).



THINSPIRATION



Trad.lett: Ispirazione al dimagrimento.

Termine che indica la promozione di comportamenti a favore dell'anoressia attraverso la pubblicazione di fotografie che rappresentano persone esageratamente magre.

Vedi: **PRO ANA**

INFORMIAMOCI

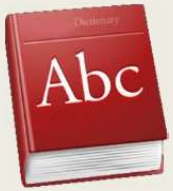
THINSPIRATION

***#thinspiration**, tra gli hashtag più popolari, mostra contenuti relativi a perdita di peso, esercizio fisico esagerato e comportamenti alimentari restrittivi. I contenuti collegati al #thinspiration sono per lo più immagini con testi che incoraggiano a non mangiare o che esprimono disagio e sofferenza, sentimenti di tristezza, isolamento, senso di inutilità, desideri di autolesionismo o pensieri suicidari. La diffusione online di contenuti pro-ana (pro-anoressia) non è recente, risalgono anzi agli anni Novanta i primi blog e siti utilizzati per promuovere condotte autolesive, diete ed esercizi estremi.*

Negli ultimi anni si è assistito a una migrazione della comunità pro-ana dai siti (statici, focalizzati esclusivamente sull'anoressia e facilmente rintracciabili dalla Polizia Postale che può chiuderli), verso piattaforme social come Instagram, più aperta e flessibile, che raggiunge velocemente un maggior numero di utenti oltre che più difficile da moderare e controllare. I divieti imposti dalle piattaforme non sono riusciti a bloccare l'attività pro-ana sui social, infatti hashtag vietati riappaiono leggermente modificati. I social network, incoraggiano inoltre l'interattività: i thinstagrammers, ad esempio, lo utilizzano in modo proattivo, ricercando automotivazione e senso di appartenenza ad una comunità che a volte viene chiamata in causa con alcuni giochi o sfide, le challenge. Si tratta di post in cui l'utente si impegna a fare o non fare alcune cose: ad esempio, digiuno o esercizio fisico eccessivo in cambio di like, o ancora chiedere ai follower di nominare un alimento che poi ci si asterrà dal mangiare per un determinato periodo di tempo. C'è anche una componente competitiva, in cui gli utenti sfidano gli altri a partecipare ai digiuni e chiedono dei #bodycheck, che consistono nel condividere peso e misure del corpo in modo che gli altri possano commentare i loro aggiornamenti, esponendosi a critiche o apprezzamenti sul loro peso.

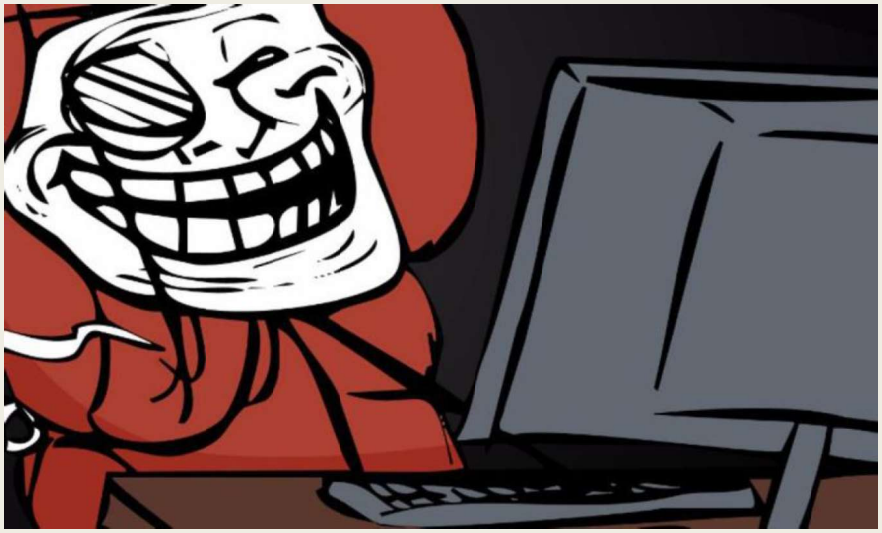
https://www.stateofmind.it/2020/01/thinspiration-socialnetwork/

Troll



Traduzione letterale: to troll, muovere un'esca in modo tale da spingere un pesce ad abboccare.
Nelle leggende scandinave, abitante demoniaco di boschi, montagne, luoghi solitari: corrisponde all'orco di altre tradizioni popolari europee.

- Trattasi di persona che scrive un commento provocatorio a un post o una frase (negativamente) mirata, al fine di generare una risposta scontrosa. Il termine è utilizzato nei news-group, nei forum, nei blog e nelle mailing list.



INFORMIAMOCI

TROLL

Di norma l'obiettivo di un troll è far perdere la pazienza agli altri utenti, spingendoli a insultare e aggredire a loro volta (generando una flame war). Una tecnica comune del troll consiste nel prendere posizione in modo plateale, superficiale e deciso su una questione vissuta come sensibile e già dibattuta dagli altri membri della comunità (per esempio una religion war). In altri casi, il troll interviene in modo apparentemente insensato o volutamente ingenuo, con lo scopo di irridere quegli utenti che, non capendone gli obiettivi, si sforzano di rispondere a tono ingenerando ulteriore discussione e senza giungere ad alcuna conclusione concreta.

"Non dare da mangiare ai Troll"

Il cross posting, ovvero la pubblicazione di un messaggio in più sezioni diverse, è un sistema utilizzato dal troll per infastidire più gruppi contemporaneamente. Un troll particolarmente tenace e astuto può scoraggiare gli utenti di una comunità virtuale fino a causarne la chiusura. La figura del troll può coincidere in alcuni aspetti con quella del fake, ovvero colui che disturba una comunità fingendosi qualcun altro. Tuttavia, un fake potrebbe partecipare in modo disciplinato e costruttivo alla conversazione (diversamente dal troll), mentre un troll potrebbe non celare né falsificare la propria identità (diversamente dal fake). Sovente le due figure, però, hanno obiettivi sovrapponibili.

Alcuni tipi di messaggi e attività associati all'azione del troll:

- L'invio di messaggi intenzionalmente sgarbati, volgari, offensivi, aggressivi o irritanti.
- L'invio di messaggi con contenuti senza senso, detto in gergo informatico flood (come: semplici parole, lettere, emoticon, testi casuali)
- L'invio di un numero di messaggi, anche se non particolarmente provocatori o insensati, tale da impedire il normale svolgimento delle discussioni.
- L'invio di messaggi volutamente fuori tema (con frasi come: "come sviluppo la mia pagina web?", in un forum nel quale si parla di musica).
- L'invio di messaggi contenenti errori portati avanti con finta convinzione (con frasi come: "Così è la vita è certamente il miglior film di Roberto Benigni, checché ne diciate!").
- L'invio di messaggi a scopo di disinformazione e critica insensata.
- Il perorare intenzionalmente e con tensione un'argomentazione basata su un errore difficile da dimostrare o su opinioni potenzialmente verosimili, facendosi seguire nella discussione dalla comunità.
- Il pubblicare contenuti di disturbo come suoni, immagini o link a siti offensivi, sovente mimetizzandoli come innocui.
- Lo svelare trame di film o libri senza avvertire (in gergo "spoilerare").
- Lo sbagliare deliberatamente e ripetutamente i nomi (di persone o cose) o regole grammaticali per irritare gli altri utenti.
- L'attribuire a tanti l'opinione di uno, vittimizzandosi e non rispondendo nel merito, spingendo possibilmente altri utenti a prendere le proprie difese (con frasi come: "vi siete coalizzati contro di me").
- Il ridicolizzare o denigrare ripetutamente gli interventi di un utente "concorrente".
- Lo scrivere deliberatamente messaggi enfatici su un dato argomento divertendosi alle spalle di chi corrobora poi la propria fasulla tesi.
- Il portare avanti tesi opposte a quelle dichiaratamente discusse nella comunità, con argomentazioni vaghe, imprecise e pretestuose, generando quindi flame (per esempio pubblicando teorie creazioniste in un forum di evoluzionisti o viceversa).

Alcune categorizzazioni tipo di Troll:

L'eccentrico ("*crank troll*")

Il martire ("martyr troll")

La scimmia dattilografa ("*infinite monkey troll*")

Il proiezionista ("*projectionist troll*")

Lo spammer ("*link spammer troll*")

Il logorante ("attrition warfare troll")

Il rancoroso ("hate troll")

Il doganiere ("*show me the passport troll*")

Motivazioni del Troll:

Secondo vari studi, sebbene comportamenti di disturbo siano riscontrabili anche nelle normali relazioni interpersonali, un ruolo chiave che spinge ad agire come troll nelle comunità virtuali è la **sensazione di anonimato** o di minore esposizione che molti utenti percepiscono durante la navigazione su internet.

Altre motivazioni sono la **ricerca di attenzione**, **divertimento o satira**, **disagio personale, combattere il conformismo, modificare l'opinione.**

https://it.wikipedia.org/wiki/Troll_(Internet)

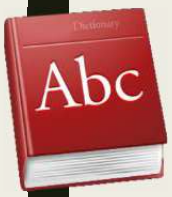
LA LEGGE DICE:

Troll comportamento a rischio

La condotta diviene criminale nei casi di:

- **art. 595 c.p. comma III** (diffamazione)
- **art. 615 bis c.p.** (interferenze illecite nella vita privata)

TYPOSQUATTING



Occupazione abusiva di spazi virtuali tramite errore di battitura

Trattasi di una forma illegale che consiste nel dirigere utenti che per sbaglio commettono un errore nella battitura dell'indirizzo URL, verso siti internet dal nome molto simile.
Spesso questa è una strategia utilizzata per diffondere malware.

Vedi anche Cybersquatting

INFORMIAMOCI

TYPOSQUATTING

Come funziona il typosquatting

Gli aggressori possono camuffare il dominio malevolo attraverso differenti metodologie:

- un comune errore di ortografia nel dominio di destinazione (per esempio gooogle.com invece di google.com);
- un dominio di primo livello diverso (utilizzando .it invece di .co.it);
- aggiunta di parole correlate nel dominio;
- aggiunta di punti all'URL (go.ogle.com);
- utilizzo di lettere dall'aspetto simile per camuffare il falso dominio (goògle.com).

È un "trucco abbastanza semplice", ma ancora enormemente efficace e redditizio per i criminal hacker.

"Riesci a vedere la differenza tra goggle.com e google.com?", probabilmente nella routine di leggere non ci accorgiamo neppure della differenza tra i due domini.

I domini malevoli possono essere utilizzati per i seguenti scopi:

estorsione: ad esempio per rivendere il dominio al proprietario del marchio;

frode pubblicitaria: monetizzando il dominio con annunci pubblicitari mostrati ai visitatori ingannati da un'ortografia non corretta, per poi reindirizzarli alla concorrenza o reindirizzare il traffico verso il marchio stesso tramite un link di affiliazione e guadagnare una commissione a ogni clic;

furto di informazioni: raccogliere credenziali e informazioni sensibili tramite e-mail di phishing o pagine di login di siti copiati;

diffamazione: raffigurare il proprietario del dominio "target" in luce negativa, una tipologia di typosquatting particolarmente comune fra i domini dei politici.

La motivazione, insomma, è quasi sempre di natura economica. L'obiettivo finale è di solito il furto di denaro, proprietà intellettuale o altri dati preziosi che possono essere venduti o conservati per il riscatto.

Il 2020 ha visto molti tentativi di spoofing di dominio con temi legati alla pandemia di COVID-19. I dati pubblicati da DomainTools ci dicono che sono stati registrati più di 150mila nuovi domini ad alto rischio, proprio a tema coronavirus, a partire dal dicembre del 2019.

Il suffisso più prezioso su internet è il .com.

Questo significa che è anche quello più prezioso per effettuare il typosquatting.

I domini più attraenti per i criminal hacker sono le istituzioni finanziarie o le organizzazioni farmaceutiche. Anche i beni di consumo di tendenza sono molto popolari come target. Motivo per il quale è sempre bene prestare particolare attenzione quando si accede a questo tipo di siti o si ricevono e-mail con link che puntano verso essi.

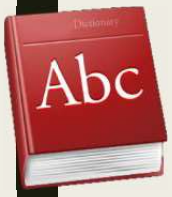
Il typosquatting è un tipo di attacco indiretto molto difficile da eludere. Banalmente, il principale "grimaldello" è la soglia di attenzione dell'utente.

Dal lato difensivo, le aziende possono anche cercare di registrare domini simili ai propri per prevenire preventivamente gli attacchi squatting e reindirizzare gli utenti all'URL corretto. Questa è tipicamente chiamata registrazione difensiva ed è una forma legittima di typosquatting. Ad esempio, Microsoft possiede più di una dozzina di domini con varianti del marchio per prevenire tali attacchi.

https://www.cybersecurity360.it/

V

VIOLAZIONE DELL'ACCOUNT



Trattasi di fenomeno complesso che comprende in particolare:
- violazione dell'account di piattaforma di commercio elettronico (o di bacheche di annunci vendita) al fine di porre fittiziamente in vendita su internet, avvalendosi di un'identità non corrispondente a quella reale, beni di varia natura con l'intento di non procedere poi all'invio dell'oggetto in questione e impossessarsi della somma di denaro;

- violazione/acquisizione indebita dell'account per accedere ai social network.

INFORMIAMOCI

VIOLAZIONE DELL'ACCOUNT

WhatsApp: il trucco incredibile con il quale rubano il vostro account

Ultimamente tramite WhatsApp alcuni truffatori sarebbero stati in grado di rubare quelli che sono gli account degli utenti. Il tutto avverrebbe in maniera molto semplice, intercettando il codice di verifica utilizzato in fase di accesso durante la connessione a WhatsApp Web. In questo modo molte persone avrebbero perso il proprio account e a segnalarlo sarebbe stata la polizia di Stato con un comunicato ufficiale:

"Molto spesso gli utenti, tratti in inganno dalla presunta conoscenza del mittente, non esitano ad assecondare la richiesta, rispondendo al messaggio, ignari di essere vittime di una truffa". Rispondendo agli hacker, "il codice inviato consente ai cybercriminali di impadronirsi dell'account WhatsApp e di sfruttare il servizio di messaggistica istantanea per compiere ulteriori frodi utilizzando il numero di telefono della vittima. Questi riescono ad avere accesso ai contatti salvati nella rubrica, innescando una sorta di catena di Sant'Antonio: il profilo WhatsApp dell'utente che ci richiede di inviargli il codice è effettivamente un nostro contatto, che a sua volta ha avuto la violazione del suo account attraverso la stessa condotta fraudolenta. Invitiamo pertanto tutti a verificare le fonti e a non cliccare mai sui link sospetti presenti nei messaggi."

https://www.tecnoandroid.it/

Come rendere più sicuro il tuo profilo Facebook

Per evitare che il tuo account sia compromesso, segui questi piccoli accorgimenti:
Scegli una password complessa e diversa per ogni account. Scegli, dunque, una password lunga, non inserire dati personali, come ad esempio date di compleanni o ricorrenze, alterna numeri e simboli. In questo modo è più difficile che la indovinino;
Attiva l'autenticazione a due fattori, attraverso questa funzione una volta che hai effettuato l'accesso, riceverai un ulteriore codice di verifica;
Attiva le notifiche per gli accessi non riconosciuti, grazie alle quali saprai se qualcuno si è collegato con il tuo account.

https://sicurezza.net/

LA LEGGE DICE:

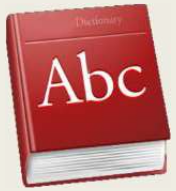
VIOLAZIONE DELL'ACCOUNT condotta criminale

art. 494 c.p. (sostituzione di persona)

art. 615 ter c.p. (accesso abusivo a un sistema informatico o telematico)

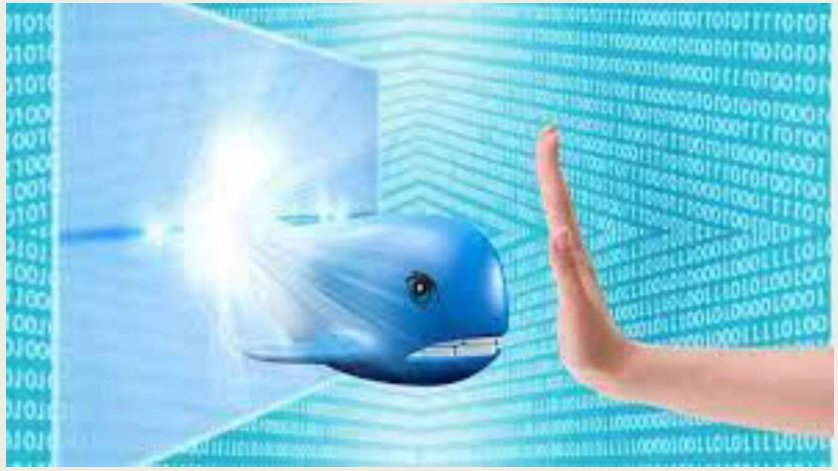
art. 615 quater c.p. (detenzione e diffusione abusiva di accesso a sistemi informatici o telematici).

Whaling



Traduzione letterale: Caccia alla balena

- Tipologia di attacco informatico che prevede l'invio di e-mail personalizzate, aumentando in tal modo la credibilità del contenuto del messaggio, al fine di truffare persone con un alto profilo professionale



INFORMIAMOCI

Whaling

Il whaling, o whale phishing, è una recente e ambiziosa tecnica di attacco informatico che prende di mira dirigenti e vertici aziendali quali CEO, CFO, CIO e in generale tutti quei profili, comunemente identificabili come C-Level, che all'interno di un'azienda sono in possesso sia di informazioni strettamente riservate che di elevati poteri decisionali e di spesa.

L'obiettivo è quello di manipolare la vittima inducendola con l'inganno a divulgare informazioni in suo possesso o a fargli compiere specifiche azioni dannose per l'azienda ma remunerative per l'attaccante, come ad esempio autorizzare un bonifico a beneficio di quest'ultimo.
Le logiche e le dinamiche di tale tipologia di attacco sono sostanzialmente le stesse del phishing, minaccia informatica particolarmente diffusa di cui il whaling rappresenta la forma più recente, evoluta e sofisticata.
In genere, essendo la vittima un soggetto ben noto, l'attaccante avrà modo di studiarne preventivamente abitudini e relazioni professionali per poi strutturare un attacco ad-hoc, aumentando esponenzialmente le probabilità di successo.
In tal senso, i social media come Facebook, Twitter e LinkedIn costituiscono una ricchissima fonte di informazioni, sia di carattere privato che professionale.
A causa delle dinamiche appena descritte, le e-mail e i siti web realizzati e utilizzati per gli attacchi di whaling possono risultare incredibilmente verosimili e, in definitiva, particolarmente difficili da rilevare anche per i profili aziendali di più alto livello.

Per contrastare il fenomeno, da parte delle aziende, occorre limitare il più possibile la condivisione di informazioni sui propri C-Level, ad esempio tramite il sito web o gli account social aziendali e da parte dei C-Level, occorre cercare di limitare la condivisione di informazioni personali e professionali, in particolare attraverso i vari social network.

https://www.cybersecurity360.it/

LA LEGGE DICE:

Whaling 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).

APPENDICE

Legislazione cyberbullismo e cybercrime

La condotte esaminate potrebbero violare alcune leggi e norme disciplinate dall'Ordinamento Giuridico Italiano, in particolare:

Art. 580 c.p. Istigazione o aiuto al suicidio: *"Chiunque determina altri al suicidio o rafforza l'altrui proposito di suicidio, ovvero ne agevola in qualsiasi modo l'esecuzione, è punito, se il suicidio avviene, con la reclusione da uno a cinque anni, sempre che dal tentativo di suicidio derivi una lesione personale grave o gravissima …".*

Art. 581 c.p. Percosse: "Chiunque percuote taluno, se dal fatto non deriva una malattia nel corpo o nella mente è punito, a querela della persona offesa ..".

Art. 582 c.p. Lesioni personali: "Se la malattia ha una durata non superiore ai venti giorni e non concorre alcuna delle circostanze aggravanti prevedute dagli articoli 583 e 585, ad eccezione di quelle indicate nel numero 1 e nell'ultima parte dell'articolo 577, il delitto è punibile a querela della persona offesa".

Art. 583 c.p. Circostanze aggravanti: "La lesione personale è grave e si applica la reclusione da tre a sette anni:SEP1) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa (1), ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;SEP2) se il fatto produce l'indebolimento permanente di un senso o di un organo …".

Art. 615 bis c.p. Interferenze illecite nella vita privata: "Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614 , è punito con la reclusione da sei mesi a quattro anni. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo….".

Art. 10 c.c: "Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni".

- **Art. 96, Legge 22 aprile 1941, n. 633**: “Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente. Dopo la morte della persona ritrattata si applicano le disposizioni del 2/a, 3/a e 4/a comma dell'art. 93”.
- **Art. 97, Legge 22 aprile 1941, n. 633**: “Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o colturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata”.
- **Art. 161, DL 196 del 2003, Omessa o inidonea informativa all'interessato**: “La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro”.
- **Art. 167, DL 196 del 2003, Trattamento illecito di dati**: “Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi”.

- **Art. 595 c.p. comma III, Diffamazione**: “Se l’offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico [c.c. 2699] , la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516 . Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o a una sua rappresentanza o ad una autorità costituita in collegio, le pene sono aumentate (c.p. 29,64)....” o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata”.
- **Art. 660 c.p. Molestia o disturbo alle persone**: “Chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo è punito con l'arresto fino a sei mesi o con l'ammenda fino a cinquecentosedici euro”.
- **Art. 612 c.p. Atti persecutori**: “Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a cinque anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumita' propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita. La pena è aumentata se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se il fatto è commesso attraverso strumenti informatici o telematici. La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona travisata. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale. La querela è comunque irrevocabile se il fatto è stato commesso mediante minacce reiterate nei modi di cui all'articolo 612, secondo comma. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d’ufficio”.

- **Art. 615 ter c.p.** Accesso abusivo a un sistema informatico o telematico: “Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la reclusione fino a tre anni.. ..”.

- **Art. 615 quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**: “Chiunque al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164. ..”.

- **Art. 615 quinquies c.p. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico**.”Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici , è punito con la reclusione fino a due anni e con la multa sino a euro 10.329”.

- **Art. 640 ter c.p. 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 a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da € 51.00 a € 1.032. …”.

- **Art. 594 c.p. comma II , Ingiuria**: "Chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa fino a cinquecentosedici euro. Alla stessa pena soggiace chi commette il fatto mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa. La pena è della reclusione fino a un anno o della multa fino a milletrentadue euro, se l'offesa consiste nell'attribuzione di un fatto determinato. Le pene sono aumentate qualora l'offesa sia commessa in presenza di più persone".

Legge 29 maggio 2017, n. 71
Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.

Punti salienti:

- Ciascun **minore ultraquattordicenne** (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media **un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella rete.** Se entro 24 il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al **Garante per la protezione dei dati personali**, che rimuoverà i contenuti entro 48 ore.
- Nasce presso la Presidenza del Consiglio dei ministri il **tavolo tecnico** per la prevenzione e il contrasto del cyberbullismo, che entro sessanta giorni dal suo insediamento redigerà un **piano di azione** integrato per il contrasto e la prevenzione del cyberbullismo. Il piano prevede anche periodiche campagne informative di prevenzione e di sensibilizzazione sul fenomeno del cyberbullismo. Entro il 31 dicembre di ogni anno, a partire dal 2018, il Tavolo farà una relazione al Parlamento sulle attività svolte.
- Entro trenta giorni dalla data di entrata in vigore della presente legge (quindi entro il 18 settembre) il MIUR adotta delle **linee di orientamento per la prevenzione e il contrasto del cyberbullismo nelle scuole**, anche avvalendosi della collaborazione della **Polizia postale e delle comunicazioni.** Le linee guida vanno aggiornate ogni due anni.
- Ogni istituto scolastico individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.
- Secondo quando già previsto dalla legge 107 (la Buona Scuola) per il triennio 2017-2019 si prevede una formazione del personale scolastico sul tema. Verrà promosso un ruolo attivo degli studenti e di ex studenti in attività di peer education, nella prevenzione e nel contrasto del cyberbullismo nelle scuole.
- I servizi territoriali, con l'ausilio delle associazioni e degli altri enti che perseguono le finalità della legge, promuovono progetti personalizzati per sostenere le vittime di cyberbullismo e a rieducare, anche attraverso l'esercizio di attività riparatorie o di utilità sociale, i minori autori di cyberbullismo.
- Il dirigente scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori dei minori coinvolti. I regolamenti scolastici dovranno prevedere esplicite **sanzioni disciplinari**, commisurate alla gravità degli atti compiuti.
- Per i minori autori di atti di cyberbullismo, fra i 14 e i 18 anni, se non c'è querela o denuncia per i reati di cui agli **articoli 594, 595 e 612 del codice penale**, scatta l'**ammonimento**: il questore convoca il minore insieme ad almeno un genitore.

CONOSCERE I RISCHI DELLA RETE CI AIUTA AD ESSERE SEMPRE CORRETTI CITTADINI DIGITALI