Anno I - numero 6 - Novembre 2020

# CODACONS Magazine

## 25 Novembre 2020

## #nonseisola

CODACONS Magazine

# Sommario




**Direttore Responsabile**
Maria Boffini
info@codaconslombardia.it

**Redazione**
Marco Maria Donzelli
Maria Boffini
Giuseppe Crusco
Valentina Danza
Nicola Castiglioni
Stefano Tiberga
Davide Carlo Sibilio
Francesca Fanunza
Irina Mullishi
Anna Del Sorbo
Enrico Venini
Carlo Gasparro
Angelo Cardarella
Nino Lisolo
Leonardo D'Onofrio
Lorenzo D'Onofrio
Emilia Macina
Alessandra Salogni
Giuseppe Puccio

**Grafica**
Davide Carlo Sibilio
Maria Boffini
Alessandro Cattaneo

**Editore**
Codacons Lombardia
Pec: codacons.lombardia@pec.it
Viale Gran Sasso, 10
20123 - Milano
tel. 02 29419096

**Facebook**
@codaconslombardiaofficial

**Instagram**
@codaconslombardiaofficial

**Ufficio Abbonamenti**
Anna Del Sorbo
info@codaconslombardia.it

**Progetto realizzato nell'ambito del Programma generale di intervento della Regione Lombardia con l'utilizzo dei fondi del Ministero dello sviluppo economico. Ripartizione 2018**

# CONSULENZA ONLINE

HTTPS://WWW.CODACONSLOMBARDIA.IT/CONSULENZE-ONLINE/

# ABBONAMENTO

# 2020

## € 60,00

LEGGI SU TELEFONO O TABLET
(ANDROID/APPLE)

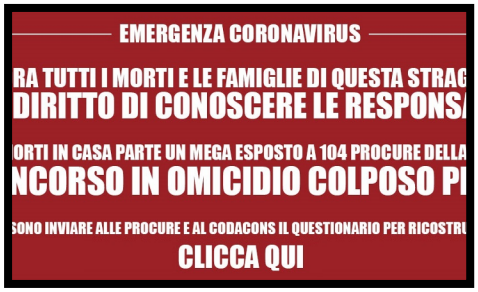
CLICCA QUI

# AZIONI CODACONS


DENTIX: ANNULLA IL FINANZIAMENTO E OTTIENI IL TUO RIMBORSO!

VIAGGI: NO AL VOUCHER, VOGLIAMO I RIMBORSI!

DERAGLIAMENTO PIOLTELLO: DALLA PARTE DEI PASSEGGERI




IL CODACONS IN PRIMA FILA CONTRO LE NEGLIGENZE NELLA GESTIONE DELLA PANDEMIA COVID-19

TRUFFA DEI DIAMANTI: AGISCI CON IL CODACONS!

# I NUMERI DEL GIOCO D'AZZARDO AL TEMPO DEL COVID-19

Lo studio GAPS#iorestoacasa condotto dall'Istituto di fisiologia clinica del Cnr di Pisa rileva il cambiamento dei comportamenti di gioco nel periodo di lock down. È stata registrata una generale diminuzione del gioco fisico, con più del 35% dei giocatori che ha ridotto le puntate e quasi il 23% che ha smesso, mentre un intervistato su tre dichiara di aver **aumentato le giocate online**. Tra gli habitué del gioco fisico il 12% ha continuato anche durante l'isolamento e circa il 10% ha puntato sul web. Le stime epidemiologiche sul gioco d'azzardo in Italia indicano che gioca per soldi metà della popolazione adulta, mentre le quote di gioco problematico hanno visto un aumento negli ultimi anni nella popolazione 15-74 anni e in particolare tra i giovani adulti.

**MA COSA È CAMBIATO DURANTE IL LOCK DOWN, CON LA CHIUSURA DEI LUOGHI FISICI DI GIOCO E LA SOSPENSIONE DI ESTRAZIONI E SCOMMESSE?**

L'Agenzia dei Monopoli evidenzia una forte contrazione della raccolta derivante dal comparto, come in tutti i periodi di crisi economica quali il 2008, d'altronde è lecito ipotizzare che la perdita di lavoro e di riferimenti spinga parte della cittadinanza a cercare fortuna proprio nell'azzardo. Sono preoccupanti le possibili implicazioni derivanti dalla chiusura di agenzie di scommesse, sale gioco e bingo e dallo spegnimento delle slot machine: la chiusura del comparto fisico dei giochi, ormai terminata, ha reso necessario monitorare le variazioni dei comportamenti, per valutare se le limitazioni abbiano favorito la migrazione verso l'azzardo online o favorito trasgressioni alle regole di isolamento.

Per tali motivi l'Istituto di fisiologia clinica del Consiglio nazionale delle ricerche (Cnr-Ifc), sollecitato dall'Associazione nazionale Comuni italiani (Anci), da alcune Regioni e da altri soggetti istituzionali coinvolti nel monitoraggio e nella prevenzione dei rischi correlati al gioco d'azzardo ha sviluppato uno strumento ad hoc per la rilevazione del fenomeno in questo particolare periodo: il questionario online GAPS #iorestoacasa. Dalle risposte date sul questionario on line, che ha raggiunto 3.971 persone in 6 settimane tra aprile e maggio 2020, emerge che il 3,6% dei rispondenti riferisce di aver giocato on-site durante l'emergenza coronavirus, principalmente presso i tabaccai, e il 3,7% riporta di aver giocato d'azzardo online. Tra chi negli ultimi 12 mesi ha giocato presso luoghi fisici, oltre un quarto dei rispondenti, durante l'isolamento il 12% ha giocato on-site e il 10,3% lo ha fatto online. I risultati del test indicano che lo studio ha raggiunto una popolazione particolarmente sensibile al tema: il 13,3% dei giocatori nell'ultimo anno e il 27,6% di chi ha giocato in periodo Covid-19, mostrano un profilo severo di problematicità, mentre sulla popolazione generale gli studi Cnr-Ifc indicano una quota di problematici intorno al 3%.

**MA COME SI SONO MODIFICATI I COMPORTAMENTI DI GIOCO DURANTE IL LOCK DOWN?**

Come atteso, lo studio rileva una generale diminuzione del gioco fisico per il 35,4% e una interruzione totale per il 22,8%. Il 26,6% riferisce di non aver cambiato abitudini e il 13,9% ha addirittura aumentato le occasioni di gioco fisico. Tra i giocatori che hanno giocato on-site nel periodo, la grande maggioranza riferisce di aver giocato al gratta e vinci (72,5%), seguono Superenalotto e Lotto. La maggioranza è uscita di casa da una a tre volte al mese per giocare, circa il 40% lo ha fatto una o più volte a settimana e l'8,5% quotidianamente, anche più volte. Se la maggior parte dei giocatori on-site ha speso non oltre i 10 euro durante l'intero periodo, il 26% ha speso tra gli 11 e i 200 euro, il 2,6% tra i 200 e i 500 euro e il 3,9% si è spinto oltre i di spesa. **Indipendentemente dai soldi spesi, il 55,3% dei giocatori on-site ammette la perdita. Per quanto riguarda il gioco online, il 33,8% riporta di aver aumentato le occasioni di gioco,**il 28,8% di non aver modificato le proprie abitudini e l'11,3% di aver iniziato in questa modalità proprio durante l'isolamento. Questi giocatori hanno preferito poker texano, slot machine virtuali e scommesse sportive online.**Nei giocatori online la frequenza di gioco è maggiore**: il 30,5% ha giocato una o più volte al giorno, altrettanti più volte a settimana, il 39% da una a quattro volte nel mese. La spesa online nel periodo in questione si rivela più consistente, con il 14,6% che riferisce di aver speso oltre 500 euro e l'11% tra i 200 e i 500 euro. Il 56,8% ammette di essere in perdita.

**Tra chi ha riportato di aver giocato on-site durante la fase 1 dell'emergenza, il 62,6% è di genere maschile, la classe di età più rappresentata è quella dei 45-54enni**e il 32,9% ha visto cambiare la propria posizione lavorativa; tra i rispondenti che hanno**riferito il gioco online il 78,6% è maschio, la classe di età più rappresentata sono i 25-34enni** e la percentuale di chi ha visto cambiare la propria posizione lavorativa sale al 52%. Sebbene queste siano le prime analisi, sembra evidente che gli habitué del gioco in luoghi fisici sono passati solo in minima parte al gioco online e che le due popolazioni di giocatori on-site e online restino ben distinte, conclude Sabrina Molinaro. Per chi fosse interessato il questionario è accessibile al seguente link.

# LA CARNE SENZA CARNE: ABUSO DI DENOMINAZIONE?

Correva l'anno 2019 e la carne "senza carne" iniziava a conquistare i *fast food* statunitensi. Startup come "Impossible foods" e "Beyond meat" si ponevano l'obiettivo di creare cibi che sembrassero carne, con il sapore della carne, con la consistenza della carne ma completamente di origine vegetale. Una perfetta idea per soddisfare le voglie "carnivore" di tutti coloro che sono vegetariani o vegani o semplicemente preferiscono un'alternativa vegetale.

**IMPOSSIBLE FOODS**

La startup fu fondata da Patrick Brown (professore presso la Standford University) nel 2011 ed ha fin da subito attirato l'attenzione di noti investitori. 75 milioni di dollari investiti che sono stati convogliati per la creazione di un centro di ricerca in California in cui veri e propri scienziati studiano gli aromi e la consistenza non solo della carne ma anche del formaggio al fine di riprodurli. *Qual è il segreto?* Il medesimo sapore della carne è dovuto **all'eme**(un complesso chimico che contiene un atomo di ferro ed è parte dell'emoglobina) che porta l'ossigeno attraverso il sistema circolatorio e rende la carne rosata.

Questa miracolosa molecola dona alla carne il suo tipico e inconfondibile sapore. L'eme è stato iniettato in un ceppo di lievito da Impossible foods.

**BEYOND MEAT**

Beyond meat è stata fondata nel 2009 in California da Ethan Brown. La società dichiara di generare meno emissioni di gas serra, utilizzare molta meno acqua e consumare meno energia rispetto alle società che producono carne animale. Beyond meat è la prima azienda di prodotti vegetali alternativi alla carne ad essere approdata in Borsa e che gode di finanziatori come Leonardo di Caprio e Bill Gates. Il primo trimestre del 2020 si è chiuso in modo decisamente positivo per Beyond Meat con un incremento del 141% rispetto ai ricavi netti dello stesso periodo dell'anno 2019. Il mercato*plant-based*si è espanso tanto che, importanti testate come Forbes, The New York Times, stanno dedicando molta attenzione al fenomeno.

**L'ARRIVO IN ITALIA DEL FAKE-BURGER**

È il 2018, proprio con Beyond meat, che arrivano questi prodotti sul suolo tricolore! È riuscito ad approdare nei menù dei 16 locali di Welldone una catena di origine bolognese che si occupa di vendere hamburger gourmet fondata nel 2013 da Sara Roversi e Andrea Magelli.

Le multinazionali che stanno osservando attentamente il mercato non hanno perso tempo! Nestlé ha lanciato l'"Incredible Burger" e ha sfidato le società americane con "Awesome Burger". Vanta di un'etichetta con meno ingredienti rispetto alle concorrenti americane. Ora consta un'intera linea *plant based* denominata "Garden Gourmet". Findus lancia la linea "Green Cuisine": burger, polpette e salsicce a base di piselli; Granarolo l' "Uncoventional burger 100% vegetale", Valsoia il "Super burger", Food Evolution gli "straccetti al gusto pollo", i "dadini gusto pancetta", etc.

**GUERRA AL PARLAMENTO EUREOPEO**

Nella seconda metà del mese di **Ottobre 2020** gli eurodeputati si sono trovati a votare sulla seguente mozione: riservare o meno la denominazione "hamburger" ma anche "salame", "mortadella", "pancetta" etc. ai prodotti a base vegetale. Le filiere dell'allevamento e dell'agricoltura hanno lanciato la campagna di sensibilizzazione "*Ceci n'est pas une steak*" (questa non è una bistecca) richiamando la celeberrima opera di*René Magritte*"*Ceci n'est pas une pipe*" con cui si ribadisce che "se non è carne non è hamburger". A livello europeo la Corte di Giustizia si è pronunciata per i prodotti lattiero-caseari vietando l'utilizzo di denominazioni come "latte", "formaggio", "yogurt" e "burro" per le alternative vegetali.


Il 23 ottobre 2020 il Parlamento europeo si è pronunciato ed ha salvato la "finta carne" ammettendo la denominazione "hamburger vegano" ma non solo! Anche le denominazioni "pancetta veg" o "prosciutto vegetale" sono ammessi. 4 sono gli emendamenti respinti:

1-La commissione agricoltura richiedeva di riconoscere come scaloppina, bistecca, salsiccia e hamburger solo prodotti a base di carne.

2-Il Ppe desiderava riservare le denominazioni utilizzate per la carne (bovino, maiale etc.), i prodotti processati della carne (salame, mortadella etc.) e i tagli della carne (fesa, braciola etc.) solo ai prodotti contenenti componenti commestibili di animali e non più del 3% di proteine vegetali ad eccezione dei cosiddetti hamburger vegetali.

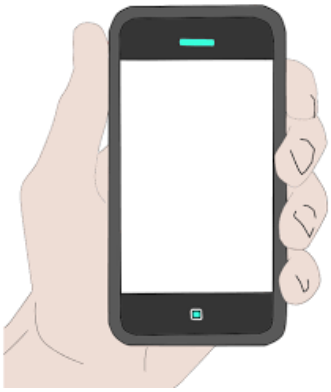
3-S&D chiedeva di riservare i nomi relativi alla carne a prodotti non vegetariani lasciando alla Commissione il potere di adottare deroghe parziali o totali alla norma;

4-Verdi/ale e Gue/ngl chiedevano che le denominazioni relative alla carne e ai tagli di carne rimanessero abbinate ai prodotti vegetali alla condizione che in etichetta fossero riportati termini che chiaramente indicassero che l'alimento in questione non contenga parti commestibili animali lasciando il via libera a denominazioni come "bistecche vegane", "veggie burger" etc.

**PERCHE' QUESTA DISTINZIONE PER I PRODOTTI LATTIERO CASEARI RISPETTO AI PRODOTTI A BASE DI CARNE O A BASE DI CARNE VEGETALE?**

La distinzione trova fondamento nel**distinguere la materia prima dal prodotto processato**. Latte, yogurt e burro sono materie prime. I burger, i salumi, il ragù sono prodotti processati che non nascono come tali.

# QUELLE STRANE PROPOSTE PUBBLICITARIE SUL CELLULARE: LO SMARTPHONE CI ASCOLTA? IL FENOMENO DEL MOBILE ADVERTISING



La pubblicità, lo sappiamo ormai da tempo, è il motore dell'economia. Tale slogan non pare più solo una "moderna" provocazione, ma proprio un dato di fatto. Infatti, negli ultimi tempi, i messaggi promozionali sembrano avere orecchie per ascoltare e motore per seguire i propri destinatari. In questo pezzo proveremo a capire in quale modo e con quali dinamiche questo "inseguimento", facente capo al Mobile Advertising, si verifichi nella nostra vita quotidiana. Il Mobile Advertising è una delle forme più moderne di pubblicità, nonché probabilmente la più invasiva tra tutte. E' infatti il mezzo attraverso cui le aziende promuovono la vendita dei propri beni o servizi ai consumatori per il tramite dello smartphone (il telefono cellulare), dei tablet e in generale dei dispositivi mobili.Il concetto di base è sfruttare l'enorme diffusione degli strumenti tecnologici portatili che ci tengono costantemente in contatto diretto con il web durante la nostra vita di tutti i giorni. E' da parecchi anni che abbiamo sostituito il vecchio e caro "telefonino" con un apparecchio utile non solo per le telefonate, ma anche e soprattutto per acquisti on-line di ogni genere, per i passatempo (videogiochi, cruciverba etc..), per rimanere in costante contatto con amici o colleghi (chat), per i social network, per la navigazione satellitare, etc, etc...

Praticamente lo smartphone è un'appendice del nostro corpo, un nuovo organo spuntato nel terzo millennio, il migliore amico inanimato dell'uomo.Il 97% per cento degli italiani sembrerebbe essere possessore di uno smartphone, dato che numericamente significa che gli smartphone nel nostro paese sono oltre 50 milioni. Numeri peraltro annualmente in crescita, così come è in crescita il tempo che i possessori dedicano al proprio oggetto tecnologico. Da qui l'idea da parte di chi vende di cercare di realizzare pubblicità calibrate su misura per ciascun navigatore del web. Facciamo un banale esempio per meglio intenderci: se un'azienda decide di pubblicizzare su un canale nazionale televisivo una merendina industriale promuovendo uno spot pubblicitario alle ore 16:00, sarà molto probabile che chi in quel momento starà guardando la tv sarà un giovane ragazzo affamato. Ovviamente gli spettatori non saranno tutti giovani ragazzi affamati, ci saranno anche le casalinghe nel loro momento di riposo, ci saranno alcuni professionisti in quel momento a letto con l'influenza etc...insomma categorie di persone potenzialmente non interessate alla merendina. Ma quanto sarebbe invece più fruttifero per un'azienda rivolgersi solo al pubblico interessato? Ebbene questa dinamica è realizzabile attraverso la veicolazione dei messaggi pubblicitari tramite smartphone (o tablet, o notebook), consistente nel rivolgere specifiche pubblicità ad un pubblico mirato (nel nostro esempio, le merendine industriali SOLO ai giovani ragazzi affamati).

Il Mobile Advertising permette di trametterе messaggi pubblicitari specifici per mezzo di banner (strisce pubblicitarie), messaggistica SMS e MMS, video, app etc… agli utilizzatori di internet. Pensateci bene. Non capita anche a voi di visitare un sito che vende auto e, dopo avere finito la ricerca ed avere cambiato pagina di navigazione in una che magari nulla c'entra con le automobili, di ritrovarvi ai bordi dello schermo pubblicità di vetture in vendita?? Se cerchiamo qualcosa su internet è ormai normale che la pubblicità di quel qualcosa ci insegua nei giorni a venire durante la nostra navigazione. Addirittura, se chiacchieriamo con un amico di un qualcosa è possibile che quel qualcosa ci sia proposta negli spazi pubblicitari on line che incontriamo nella nostra navigazione sul web. Dunque la domanda nasce spontanea: come fanno a sapere quale pubblicità indirizzare a ciascuno di noi? In primis con i "cookie", i file di testo che accettiamo ogni volta che navighiamo e che memorizzano le nostre preferenze per un determinato sito (e dunque prodotto o servizio) e più in generale la nostra cronologia di navigazione. Inoltre quando accediamo ad un sito non creando una specifica password ma usando il nostro "account" social (Facebook, Google, etc…). Ed ancora attraverso i cosiddetti "Facebook pixel" (Facebook, ma anche Instagram, Google ed altri) un codice genetico telematico di noi stessi scaturente dalle informazioni relative ai "like" che mettiamo, ai video o status che condividiamo, agli articoli che leggiamo etc…

Questi i metodi più diffusi, ma non i soli, per conoscere i nostri gusti, la nostra geolocalizzazione, le nostre preferenze, i nostri orientamenti, le nostre vacanze e così di seguito. Lo smartphone sa tutto di noi, persino che banca abbiamo e, volendo (non senza che ciò sia illegale) magari anche il nostro conto in banca. Conosce i nostri orientamenti sessuali e persino se siamo, o meno, fedeli nei confronti del nostro partner. Il problema probabilmente sta nel concedere queste informazioni troppo a cuor leggero. Lo svago, si sa, è un momento in cui si svorrebbe per qualche manciata di minuti poter staccare la spina, ma il web rappresenta un mare minaccioso, se non per rischi fisici, quantomeno per rischi relativi alla nostra preziosa privacy che, sempre di più, cerchiamo di tutelare. Conoscere queste dinamiche certo non risolverà il problema dell'assalto costante ai nostri dati, ma probabilmente ci potrà permettere di constatare l'esistenza del fenomeno e, si auspica, di prendere in futuro decisioni con più consapevolezza.

# 25 NOVEMBRE 2020

# #NONSEISOLA

Il 25 Novembre non è una data qualunque… è la giornata internazionale contro la violenza sulle donne. È importante ricordare queste vittime non solo il 25 Novembre ma in tutti i giorni dell'anno ma scopriamo insieme perché è stata scelta proprio questa data… Istituita nel 1999 segna il ricordo di un brutale omicidio commesso nel 1960 nella Repubblica Domenicana. Siamo ai tempi del dittatore Trujillo e le tre sorelle Mirabal, considerate rivoluzionarie, furono vittime di tortura, massacro e vennero infine strangolare. Le salme vennero gettate in un burrone per simulare un incidente. Siamo nel 2020, più di mezzo secolo è passato ma nel mondo i fatti non sono cambiati. Nel mondo, pensiamo alle migliaia di bambine indiane che giornalmente sono vittima di stupro e violenza ma non solo, pensiamo a noi, a quella conoscenza che abbiamo, a quel fatto di cronaca riportato sul quotidiano fresco di stampa. Poche le violenze palesi, troppe le violenze nascoste e dove? Dove si dovrebbe poter essere l'espressione di sé stessi al 100%, dove dovrebbe essere il nostro luogo sicuro. La violenza, purtroppo, si consuma per la maggior parte nel luogo che dovrebbe essere più a noi sicuro: la casa. Ed è così che l'ONU con la risoluzione 54/134 del 17 dicembre del 1999 istituiva la Giornata internazionale per l'eliminazione della violenza contro le donne. Violenza non è solo l'abuso fisico ma anche quello psichico. Violenza è anche 1,00 euro in meno di stipendio rispetto al collega maschile che svolge il medesimo compito. Violenza è un apprezzamento malizioso effettuato da uno sconosciuto quando si sta solo "camminando per strada". Violenza è non poter mettere un vestito che piace solo perché "chissà cosa penserà il mio ragazzo", "chissà cosa penseranno le persone"… solo per il fatto che nella donna si innescano certi pensieri la violenza, la disuguaglianza si commette. Spesso si discute sul termine "femminicidio" perché incostituzionale. Lede il principio di uguaglianza sancito dall'art 3 della Costituzione della Repubblica. Ma guardiamo i fatti: ancora oggi le donne sono vittime di disuguaglianza sociale al di fuori e al di dentro delle mura domestiche. "la donna pulisce", "la donna stira", "la donna esegue le faccende": disuguaglianza. La violenza peggiore è quella commessa dalle persone che si amano: uno schiaffo e poi… "scusa"; "ma come ti vesti!"… "non era una critica ma è perché sei troppo bella e sono geloso" "non devi uscire stasera"… "non pensare male ma è perché ci tengo che non ti stanchi" Un pugno e "ti sembra l'ora di tornare!"… "scusa ero solo preoccupato". Ed ecco che la violenza si consuma… una botta giustificata per paura di dire che è stato l'amore della propria vita a procurarlo. Una violenza psicologica…la peggiore… che innesca nella donna un senso di colpa… un senso di essere "sbagliata", un senso di pensare "in fondo ha ragione".

Ma non è così! Donne non siete sole fate sentire la vostra voce, dite no alla violenza! Fuori c'è un mondo di uomini e donne pronte ad aiutarvi a sostenervi a darvi l'amore vero. Una piccola ricerca in Google e migliaia di centri di aiuto per donne maltrattate. Purtroppo, spesso vi sono anche dei figli che devono subire le violenze del padre effettuate sulla propria madre ed è così che anche loro diventano vittime di violenza. Ed è così che si instaura un circolo vizioso un circolo che può costringere il bambino ad assistere al funerale della propria madre... cosa che non dovrebbe accadere. Facciamo sentire la nostra voce diciamo NO ALLA VIOLENZA! In base ai dati aggiornati dall'ISTAT il 31,50% delle 16-70enni (6 milioni) è stata vittima di violenza fisica e sessuale. 2.000.800.000 donne han subito violenza fisica e sessuale dal proprio partner o ex partner. Le donne subiscono minacce (12,3%), sono spintonate o strattonate (11,5%), sono oggetto di schiaffi, calci, pugni e morsi (7,3%). Altre volte sono colpite con oggetti che possono fare male (6,1%). Le forme più gravi di violenza sono esercitate da partner, parenti o amici. Gli stupri sono stati commessi nel 62,7% dei casi da partner. Oltre alla violenza fisica o sessuale le donne con un partner subiscono anche violenza psicologica ed economica: comportamenti di umiliazione, controllo ed intimidazione, svalorizzazione e privazione o limitazione nell'accesso alle proprie disponibilità economiche o della famiglia.
Le donne uccise sono una ogni tre giorni e, in lockdown in 4 casi su 5 l'omicida è il convivente. Il lockdown ha accellerato il femminicidio. Osservando i dati i casi durante il lockdown si sono addirittura triplicati arrivando ad un caso ogni due giorni.

## IL CODICE ROSSO

La legge Codice rosso si pone l'obiettivo di garantire una maggiore tutela alle vittime di violenza domestica e di genere. Fu la legge n. 69/2019 conosciuta come "Codice Rosso" a rafforzare la tutela delle vittime di violenza di genere e domestica inasprendo la repressione attraverso interventi modificativi in materia penalistica (codice penale e codice di procedura penale). Il testo è composto da 21 articoli nella quale sono evidenziati i reati attraverso i quali si esercita la violenza domestica e di genere. La legge si pone l'obiettivo di velocizzare l'instaurazione del procedimento penale e l'accelerazione dell'adozione di provvedimenti posti a protezione delle vittime. All'art 612-ter c.p. viene introdotto il reato di Revenge Porn con cui si puniscono le condotte di coloro che inviano, consegnano, cedono, pubblicano o diffondono senza l'esplicito consenso della persona interessata immagini o video a contenuto sessuale esplicito destinati a rimanere privati. La pena si applica anche a chi, avendo ricevuto o comunque acquisito le immagini o i video, li diffonde al fine di recare nocumento agli interessati. La fattispecie risulta aggravata se i fatti sono commessi nell'ambito di una relazione affettiva, anche cessata, o con l'impiego di strumenti informatici, nonché in danno di persona in condizione di inferiorità fisica o psichica o di una donna in stato di gravidanza. Viene introdotto, all'art. 583-quinquies cp il delitto di deformazione dell'aspetto della persona attraverso lesioni permanenti al viso.

A fronte di notizie di reato relative a delitti di violenza domestica e di genere, si prevede che la P.G., riferisca immediatamente al pubblico ministero, anche in forma orale. Alla comunicazione orale seguirà senza ritardo quella scritta. Il pubblico ministero, entro 3 giorni dall'iscrizione della notizia di reato, assumerà informazioni dallapersona offesao da chi ha denunciato i fatti di reato. Tale termine potrà essere prorogato solo in presenza di imprescindibili esigenze di tutela di minori o della riservatezza delle indagini, anche nell'interesse dellapersona offesa. La polizia giudiziaria procederà senza ritardo al compimento degli atti di indagine delegati dal PM e, metterà a disposizione del PM la documentazione delle attività svolte. Inasprita anche la pena in tema di maltrattamento con famigliari e conviventi ex art. 572 c.p. che diventa quella della reclusione da 3 a 7 anni e non più da 2 a 6 anni. Una novità importante emerge dalla modifica della misura cautelare del divieto di avvicinamento ai luoghi frequentati dalla persona offesa in modo da garantire il rispetto della misura coercitiva attraverso il braccialetto elettronico.

## IL SIMBOLO DELLA SCARPA ROSSA

Correva il 27 luglio 2012 quando Elina Chauvetle utilizzò per la prima volta in un'installazione artistica pubblica davanti al consolato messicano di El Paso, in Texas, per ricordare le centinaia di donne uccise nella città messicana di Juarez.

L'artista che visse in Messico negli anni della formazione universitaria constatò il fenomeno della sparizione di alcuni giovani donne rinvenute senza vita nel deserto. Tutterapite, stuprate, mutilate e uccise per strangolamento. Chauvet rilevo come la città e le autorità minimizzassero il problema e dietro alle ragazze brutalmente uccise vi erano studentesse e lavoratrici delle Maquiladoras (fabbriche che impiegano manodopera a basso costo). L'artista a questo punto decise di interrompere il silenzio e, nel 2009, ha raccolto 33 paia di scarpe installandole nello spazio urbano di JuArez. Dopo due ann,i ripeté l'iniziativa a Mazatlan per cui vennero donate 300 scarpe e da quel giorno le scarpette rosse, simbolo del sangue versato dalle donne vittime di violenza, sono divenute simbolo della Giornata Internazionale contro la violenza sulle donne.

# PIOGGIA DI ACCREDITI NON AUTORIZZATI SULLE CARTE DI CREDITO? OCCHIO AL VISHING.

**Il vishing è una pratica relativamente nuova in Italia, mentre negli Stati Uniti impazza da molti anni, ma cerchiamo di capire di cosa si tratta.** Il vishing o phishing vocale **si verifica quando un truffatore crea un sistema vocale automatizzato (o manuale) per fare chiamate vocali verso utenti telefonici e chiedere loro informazioni private.** L'intento è lo stesso del phishing di e-mail o dellosmishing: il truffatore, fingendosi un operatore bancario, con una chiamata vocale crea un senso di urgenza (con la scusa di un blocco del conto per operazioni sospette) per l'utente che per questo motivo fornisce informazioni riservate.

**ATTENZIONE! NON FORNIRE MAI ALCUNA INFORMAZIONE AL TELEFONO, NEPPURE SE IL NUMERO CHE CI CHIAMA E' IL SOLITO NUMERO DELLA BANCA!**

**Occorre sottolineare infatti** che è facile per un truffatore creare un ID di chiamata falso spacciandosi per qualcun altro. Esistono molte tipologie di chiamate che veicolano truffe di tipo vishing, da quelle che vogliono "appiopparci" un nuovo contratto esasperandoci e facendo leva sul risparmio, a quelle che lo fanno totalmente a nostra insaputa. Fino ad arrivare a chi intende truffarci seriamente, richiedendo i nostri dati relativi al conto corrente o alla carta di credito, o carpendo e incrociando dati sensibili in giro per Internet, che noi, a volte del tutto inconsciamente, abbiamo lasciato nel corso degli anni. O, ancora più probabilmente, incrociando dati da banche dati lecite, tramite però delle "talpe", ovverosia avvalendosi di personale (spesso pubblico) corrotto che, in cambio di poche centinaia di euro, è in grado di scovare quei dati.

**Il ruolo dei call center**

Nell'anno appena trascorso sono stati accertati casi clamorosi delle maggiori società di telefonia italiana le quali, indirettamente, ovvero affidando mandati a società "terze", falsavano dei contratti. Tutto molto semplice: l'operatore telefonico, durante la chiamata, poneva delle domande personali al cliente; così facendo, quando il cliente rispondeva quel fatidico e aspettato sì, l'operatore telefonico lo registrava e lo usava in un secondo momento per la stipulazione del contratto telefonico. Naturalmente questo non è affatto legale, ed è anche molto subdolo come sistema. Però, a dispetto della legalità, i contratti sono comunque validi. Per recedere, il modo migliore è quello di chiedere copia della registrazione vocale alla società in oggetto. Se l'azienda non accoglie la richiesta dell'utente che chiede copia della registrazione con cui ha effettuato un ordine telefonico, commette un illecito e ci si può rivolgere al Garante della Privacy per ottenere soddisfazione. Se si disconosce il presunto consenso all'attivazione di un servizio, si deve procedere immediatamente con la richiesta di disattivazione senza oneri, richiedendo anche copia della registrazione vocale al gestore (per raccomandata A/R.).

Se non si ottenessero riscontri, occorre denunciare il fatto al Garante della privacy.

### Il furto di carte di credito e conti correnti

C'è stata un'impennata relativamente ai reati di associazione per delinquere finalizzata alla sostituzione di persona, al furto aggravato e all'indebito utilizzo di carte di pagamento elettronico. Le modalità con cui avviene questa particolare tipologia di truffa sono abbastanza riconoscibili. Chi chiama, tramite un numero praticamente identico al solito numero conosciuto e utilizzato dalla propria banca, dice di appartenere ad un istituto di credito e riferisce al cliente che la propria carta è stata oggetto di un tentativo di truffa. Per "sventarlo" vengono quindi chiesti alcuni dati sensibili, come ad esempio il pin della carta, con cui poi i truffatori possono avere libero accesso al credito. Spesso le difese della vittima vengono abbassate dal fatto che la voce dall'altra parte della cornetta è a conoscenza del numero della carta, che nella maggior parte dei casi viene carpito con furti mirati. Nella maggior parte dei casi si tratta di telefonate preregistrate fatte attraverso servizi VoIP di internet (voice over IP, ossia telefonia via Internet, la stessa tecnologia impiegata da Skype e simili, per intenderci). Ma ci sono anche chiamate in diretta, con operatori in carne e ossa. a tipologia di telefonata prevede la comunicazione di un qualche problema sul conto bancario o sulla carta di credito e suggerisce di telefonare a un certo numero per risolverlo.


Facendolo, una voce automatica chiede di fornire i dati sensibili. Un altro possibile caso. Il raggiro inizia con una telefonata tradizionale, da parte di una finta finanziaria: "Crediamo che lei sia rimasta vittima di una truffa durante una transazione con la sua carta di credito. È questo il suo numero di carta di credito?". Quando si sente che l'interlocutore conosce il numero di carta, si è portati a rispondere "Sì, è questo il numero ". Viene confermata anche la data di scadenza, nota al telefonista. E si è spinti a rivelare, quasi automaticamente, anche quello che dovrebbe essere taciuto: il codice di sicurezza della tessera.

### I consigli per difendersi dal phishing vocale

Come abbiamo visto, è semplice, sull'onda emotiva, che ci vengano "estorte" informazioni sensibili. Il consiglio più importante, oltre all'ovvio (non fornire mai password, PIN, CVC o altro a nessun interlocutore) è quello di non effettuare mai bonifici a terzi se non si ha la certezza della loro identità. Prendere mentalmente nota della società che ci sta chiamando e ritelefonare subito dopo, utilizzando i canali ufficiali (ovvero dai numeri presenti dal loro sito Web ecc.). Non è detto che chi ha telefonato sia chi dice di essere: può aver trovato alcune informazioni sui Social e le altre le ha desunte oppure gliele abbiamo inconsapevolmente fornite. Utilizzando queste accortezze, tuttavia, ciò potrebbe non essere di per sé sufficiente ad evitare operazioni truffaldine sul proprio conto corrente o tramite la propria carta di credito. Nel caso ciò accadesse, infatti, ci si può sempre rivolgere ad un'associazione dei consumatori, con legali esperti della tematica, in grado di farvi riavere il maltolto.

# DIGITAL KIDNAPPING: FURTO ONLINE DI FOTO DI BAMBINI E NON SOLO.

La tutela dei minori, in particolare dei bambini, assume un gran rilievo quando si tratta dell'utilizzo inconsapevole della rete. Accanto ai noti fenomeni, come il cyberbullismo, si aggiunge il digital kidnapping, ossia, un vero e proprio "rapimento digitale" attraverso il quale, i cybercriminali duplicano l'identità per finalità più disparate, utilizzando i dati e le informazioni, dei nostri figli e della famiglia, che noi stessi decidiamo di mettere online. Spesso gli adulti non si rendono conto che, la condivisione compulsiva di immagini dei propri figli, ad esempio, l'ecografia, i compleanni, la passeggiata al parco, rilevano dettagli che possono essere sfruttati da malintenzionati per svariati fini. Quindi, come proteggerci e proteggere la loro incolumità fisica e psicologica. Innanzitutto, cerchiamo di capire più da vicino il fenomeno del digital kidnannige poi ci soffermeremo sulle modalità di protezione dei dati e informazioni che pubblichiamo online.

**Che cos'è il digital kidnapping**

Letteralmente *digital kidnapping* significa "rapimento digitale" e ci si riferisce al comportamento con quale una persona ruba la foto di un minore online e la pubblica come se fosse la propria. Ciò può riguardare non un singolo dato, ma un insieme di informazioni finalizzate a creare "un'identità digitale alternativa" della persona stessa. Codesta pratica consente ai cybercriminali di acquisire dati e fotografie di bambini, creare nuovi profili, per così entrare in contatto con altri minori sui social network. Sono numerose le persone che pubblicano foto dei propri figli in diversi momenti della propria vita. Queste immagini se da un lato sono un ricordo importante per i genitori, parenti e amici, dall'altro può fornire a un cybercriminale i mezzi necessari per scoprire le informazioni personali, talvolta anche sensibili, dei bimbi. Con la condivisione di questi dati online, è pertanto facile a un criminale rintracciare i dati e mettere insieme tutti i pezzi per poter colpire. Oltre ai rischi legati alla condivisione fuori controllo delle immagini dei propri bambini e l'uso criminale che può essere fatto di esse online, possono anche sorgere **rischi concreti per la sicurezza fisica dei bambini.** In questo modo, molte foto innocenti di minori condivise dai propri genitori finiscono per ritrovarsi su **siti a carattere pedopornografico**. Se si aggiunge la relativa facilità, come accennato, con la quale si possono rintracciare informazioni personali a partire da una semplice foto condivisa ingenuamente online, le persone malintenzionate non avranno nessuna difficoltà per localizzare e contattare i bambini utilizzando profili creati anonimi o creati a tale scopo. Questo non significa che è assolutamente vietato condividere foto dei propri figli con il suo network sui social ,ma va fatto con la consapevolezza dei rischi incorsi e adottando le giuste cautele.

**Come proteggersi dai rischi del digital kidnapping?**

Non esiste la sicurezza perfetta sulla rete. Tuttavia,esistono diverse misure da tenere presenti quando si pensa a condividere foto, e quindi dati personali, su un social network soprattutto quando ritraggono bambini o minori. In primis, è fondamentale **limitare l'accesso ai propri profili social** e quindi alle foto condivise. È possibile, ad esempio, definire impostazioni più rigorose su questi profili, ad esempio limitando la visibilità dei post ai soli amici o rendendo invisibile al pubblico le foto di copertina e di profilo. Poi, anche definendo impostazioni privacy più rigorose, è pur sempre essenziale **essere selettivi nelle immagini che vengono condivise** e quindi limitare il numero di foto dei propri figli online. Inoltre, costituisce sempre una buona pratica fare attenzione a ogni piccolo dettaglio tutte le volte in cui utilizziamo un social network. E' infatti possibile rintracciare il luogo dove è stata presa una foto analizzandone i minimi dettagli. Infine, si deve avere in mente che **nulla viene veramente cancellato dal web**. Pertanto, prima di postare bisogna riflettere sull'impatto e sul danno che un post potrebbe avere su un bambino in crescita. In conclusione, se è diventato parte della nostra vita oggi condividere ogni singolo momento che si ritiene importante, **non devono essere trascurati i rischi della condivisione massiccia di quelli che in realtà sono dati personali**, soprattutto quando riguardano i propri bambini. Il digital kidnapping, ovvero il furto di foto anche di bambini online, non solo può causare danno all'immagine e alla reputazione digitale degli stessi, ma può avere ripercussioni drammatiche sulla loro sicurezza fisica e psicologica.

Ed è per questo che, sebbene sia di estrema rilevanza stabilire impostazioni privacy rigorose sui propri profili, nonché limitare al massimo le informazioni che possono essere acquisibili dalle immagini condivise online, di altrettanto se non superiore importanza è la presa di conoscenza, degli adulti in primis, dei sempre maggiori rischi e delle minacce di cui la rete costituisce veicolo principale. Infatti nessuna impostazione o accorgimento tecnico potrà mai sostituire una cultura consapevole della protezione delle informazioni che ci riguardano, e che si riferiscono, in particolare a bambini e adolescenti.

# ABBONAMENTO

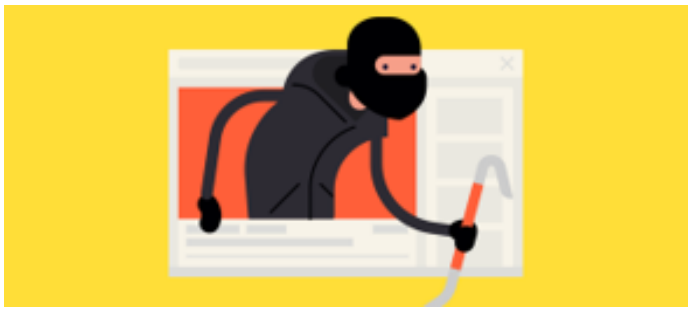
# 2020

## € 60,00

LEGGI SU TELEFONO O TABLET
(ANDROID/APPLE)

**CLICCA QUI**

# COS'È E COME È REGOLATO IL CYBERSQUATTING



Il cybersquatting (o domain grabbing) è un fenomeno comparso sulla scena sociale di pari passo all'avvento e diffusione di internet. Il fenomeno è nato negli Stati Uniti sul finire degli anni '90 e il termine deriva dall'inglese squatting, parola con cui si designa il fenomeno dell'occupazione di terreni o edifici abbandonati, di solito motivata da finalità ideali o sociali. Il cybersquatting, similmente, è una sorta di occupazione di nomi a dominio solitamente corrispondenti o simili a marchi noti. Volendo fornirne una definizione esso consiste nel registrare o utilizzare un dominio web in malafede con il fine di cercare di ricavare un guadagno economico da marchi registrati ed appartenenti ad un altro soggetto. Il cybersquatter ottiene infatti, ingenti guadagni dalla vendita di un dominio regolarmente registrato a coloro che detengono i diritti sulle firme sfruttate.
Un esempio può essere utile a chiarire come opera il cybersquatter e da dove provenga il suo guadagno. Si ipotizzi che la società "X", mediti il lancio di un prodotto denominato "Y"; a causa di un leak di informazioni mesi prima del lancio il cybersquatter acquista immediatamente tale dominio che la compagnia non aveva registrato per poi rivenderlo alla società "X" ad un prezzo molto più alto rispetto ai costi di registrazione. Secondo un report del 2009 dell'Organizzazione mondiale per la proprietà intellettuale (Wipo) dell'Onu nei 10 anni precedenti oltre 14 mila casi di cybersquatting sono stati sottoposti alla sua attenzione; nel solo 2008 le denunce erano state oltre 2mila circa il 18% in più rispetto al 2006 e il 48% in più rispetto al 2005. Tra le vittime, la Fifa e Scarlett Johansson, ma anche l'università di Yale, Google e il BlackBerry, i siti sulla candidatura di Madrid per le Olimpiadi 2016, ma anche la Bbc, così come l'Arsenal footbaal club e nomi di aziende quali eBay o Nestlé. Celebre il caso, in ipotesi perfettamente legale, di Rick Schwartz, noto con il soprannome di domain king, che nel corso degli anni ha registrato o acquistato circa 3mila nomi di siti internet estremamente comuni, prevedendo in anticipo l'importanza che questi avrebbero avuto e rivendendoli a peso d'oro. Nel 1997, ha acquistato per soli 42mila dollari, il dominio porno.com, ceduto nel 2015 per 8 milioni di dollari (dopo aver guadagnato quasi 10 milioni in pubblicità).

Insomma, quello del cybersquatting, è un fenomeno di sempre maggiore attualità e destinato, nelle stime, ad aumentare sempre più il suo peso specifico negli anni a venire. Quello richiamato nell'esempio è, tuttavia, solo uno dei casi di cybersquatting; se ne possono individuare diversi, infatti, a seconda di come lo schema base viene alterato. Annoveriamo pertanto il **Cybersquatting con intento criminoso**. Si tratta della tipologia più comune; il cyber criminale registra il dominio con il solo scopo di ottenere un ricavo monetario, rivendendolo al legittimo proprietario dei diritti sul marchio. Da questo possiamo distinguere il **Typosquatting/punycode**. In questa variante il cyber criminale registra un dominio con un piccolo errore ortografico nel nome rispetto al dominio originale (ad esempio, www.XYZ1.it in luogo di www.XYZ.it), quindi crea un sito di phishing che può essere utilizzato per spingere l'utente a condividere dati personali o a scaricare software contenente malware. Vi è poi il c.d.**Gripe sites**. Si tratta di siti web creati ad hoc per schernire ed offendere persone, politici e grandi compagnie. Sul sito Webgripesites è elencata una serie di siti web contro i quali sono state intraprese azioni legali. Da notare che, comunque, i gripe sites possono essere talvolta legittimi, cioè quando ciò che viene trattato non è diffamante nei confronti del detentore dei diritti sul marchio utilizzato per comporre il nome del dominio. Ancora, vi è il **Name jacking**. Il cyber criminale procede, in questo caso, all'acquisto di un dominio con il nome di una persona, ad esempio, per Roberto Lanfranchi, robertolanfranchi.com. Ciò permette, creando un opportuno sito, di dirigere le ricerche per tale persona al portale. Si possono immaginare chiaramente le conseguenze nel caso in cui il name jacking avvenga nei confronti di personaggi noti: gli utenti sarebbero spinti a visitare il sito web, generando traffico e venendo esposti a pericolo di phishing. Non bisogna, infine, dimenticare il classico **Furto d'identità**. I cyber squatter, in questa variante, possono utilizzare tool automatizzati per acquistare i domini non rinnovati in seguito alla scadenza della registrazione. Se il legittimo proprietario non procede al rinnovo, il dominio diviene pubblicamente disponibile. Appare evidente come sia possibile difendersi dal cybersquatting solo adottando una particolare serie di accortezze. In particolare: registrare i propri marchi presso l'Ufficio Brevetti e Marchi e verificare la scadenza dei propri domini e rinnovarli, onde non consentire l'acquisto da parte di terzi.

Se ci si avvale di un servizio esterno per la creazione di un sito o per l'assistenza, è importante che la registrazione del dominio non venga mai delegata a tale servizio. Potrebbe essere utile anche avvalersi del rinnovo automatico della registrazione del dominio, se disponibile. Al di là di queste accortezze una domanda sorge spontanea: il cybersquatting è legale? La risposta è: evidentemente no in larga parte dei casi. Il comportamento del cybersquatter impatta su diversi diritti e interessi: ne è inficiato il mercato, il cui sistema concorrenziale viene esposto a pratiche commerciali scorrette; ne è leso il titolare del marchio, al quale viene preclusa la possibilità di registrare e di utilizzare il proprio domain name; ne sono lesi i consumatori, ingannati o truffati. Al contempo, viene agevolato il perseguimento di ingiusti profitti al cybersquatter. Cerchiamo quindi di capire quali sono le conseguenze giuridiche del cybersquatting nell'ordinamento italiano. In primo luogo, l'art. 22 del Codice della proprietà industriale, nel disciplinare l'unitarietà dei segni distintivi, fa espresso divieto di adottare come nome a dominio di un sito usato nell'attività economica un segno uguale o simile all'altrui marchio, laddove possa determinarsi un rischio di confusione per il pubblico, causato anche della mera affinità tra l'attività di impresa dei titolari del marchio ed il nome a dominio adottato. Tale sistema di tutela affianca quella più ampia (cd. ultramerceologica) di cui gode il marchio che goda nello Stato di rinomanza (co. 2). Il soggetto che si ritenga leso nei propri diritti e che voglia riappropriarsi dello spazio web di sua spettanza, potrà avvalersi di diversi rimedi: sia di carattere giudiziale, sia rientranti nelle cosiddette ADR (Alternative Dispute Risolution). Tra i primi ricadono le fattispecie previste dal Codice della proprietà industriale agli articoli 118, che al comma 6 introduce il rimedio della revoca e del trasferimento del nome a dominio registrato in violazione dell'art. 22, e 133, che disciplina il rimedio cautelare dell'inibitoria e del trasferimento provvisorio. Tra gli strumenti alternativi di risoluzione delle controversie, invece, occorre menzionare l'arbitrato irrituale e la procedura di riassegnazione, da tenersi dinanzi al Registro Italiano (ente delegato dall'ICANN, cui compete l'aggiornamento di database dei nomi a dominio assegnati), in grado di conciliare effettività della tutela, speditezza della procedura e costi contenuti. Al titolare di marchio spetta altresì la tutela prevista dall'art. 2598 Codice Civile, a presidio degli illeciti concorrenziali, nonché la tutela risarcitoria di cui all'art. 125 Codice Proprietà Industriale. Come visto, tuttavia, la cifra di illiceità della condotta del cybersquatter non si esaurisce nella lesione di interessi privati e pertanto necessita di presidi di carattere pubblicistico.

L'Autorità Garante della Concorrenza e del Mercato (AGCM) ha avuto modo di occuparsi della fattispecie de qua ed ha reputato la condotta del professionista, consistente nella registrazione ed utilizzazione di un nome a dominio, in assenza di qualunque rapporto con l'omonimo operatore, idonea ad assurgere a "pratica commerciale scorretta", nella sub specie della pratica ingannevole, esplicitamente vietate ai sensi del Codice del Consumo (AGCM, 9 ottobre 2012 n. 23976). In particolare, la condotta del cybersquatter è stata ritenuta sussumibile nelle fattispecie descritte agli artt. 20, comma 2, 21, comma 1, lett. f) e 23, lett. o) del Codice del Consumo, per le quali:

-una pratica commerciale è scorretta se contraria alla diligenza professionale ed idonea a falsare il comportamento economico del consumatore medio (art. 20 co. 2);

-una azione è ingannevole se idonea ad indurre in errore il consumatore medio in ordine alla natura, qualifica e diritti del professionista, quali l'identità, il patrimonio, le capacità, lo status, il riconoscimento, l'affiliazione o i collegamenti e i diritti di proprietà industriale, commerciale o intellettuale (art. 21 co. 1 lett f);

-una azione è ingannevole ove volta a promuovere un prodotto simile a quello fabbricato da un altro produttore in modo tale da fuorviare deliberatamente il consumatore inducendolo a ritenere, contrariamente al vero, che il prodotto è fabbricato dallo stesso produttore (art. 23 lett. o).

La rilevata violazione ha indotto l'AGCM a disporre l'applicazione della sanzione amministrativa pecuniaria di cui all'art. 27 Cod. Cons., nel caso quantificata nella misura di Euro 10.000,00.

# CONSULENZA ONLINE

HTTPS://WWW.CODACONSLOMBARDIA.IT/CONSULENZE-ONLINE/

# SMS POSTE, TRUFFE IN AGGUATO

**Un nuovo modo di truffare**

Con maggiore frequenza arrivano agli utenti messaggi sulla mancata sicurezzawebdel proprio profilo utente: trattasi della nuova truffa che gira sui cellulari da un mese a questa parte. Anzitutto, Poste Italiane S.p.A. non chiede mai i propri dati riservati in nessuna modalità e per nessuna finalità. Nell'ottica, dunque, di rendere l'utente consapevole del rischio di frodi e raggiri da parte di terzi, analizziamo più nel dettaglio in che cosa consiste questo tipo di truffa e il modo in cui avviene. Di solito, arriva un sms all'utente con scritto "Le sue utenze postali saranno sospese per mancanza sicurezza*web*– Le aggiorni al*link*..". Aprendo il *link*, tuttavia, viene richiesto di inserire tutta una serie di dati personali destinati esclusivamente a colui che ha inviato l'SMS: il truffatore. Mentre in precedenza il mittente truffatore era un certo "POSTE ID", adesso è diventato POSTE INFO. In questo modo l'utente è ingannato, pensando di ricevere un sms da Poste Italiane S.p.A.; in realtà, anche se la forma sembra essere quella ufficiale, il contenuto è completamente falso e riferibile al tentativo di appropriarsi dei vostri dati personali.

Anzitutto, è bene chiarire che Poste Italiane S.p.A. e PostePay S.p.A. non chiedono mai i vostri dati personali in nessuna modalità e per nessuna finalità; di conseguenza, qualora qualcuno dovesse chiedervi informazioni di questo tipo, si tratta di un tentativo di truffa. Per questo motivo, è bene non rispondere mai a e-mail, sms, chiamate o chat, anche da call center, in cui vi vengano chiesti i vostri codici personali.


1) Non scaricare mai allegati delle e-mail sospette prima di avere verificato che il mittente sia noto o ufficiale;

2) Controllare sempre l'attendibilità di una e-mail prima di aprirla (per esempio, controllare l'indirizzo e-mail del mittente e verificare che sia realmente chi dice di essere);

3) Non cliccare sul *link* contenuto nelle e-mail sospette.

4) Segnalare a Poste Italiane le e-mail ricevute inoltrandole all'indirizzo antiphishing@posteitaliane.it, e poi cestinarle.

**Se siete vittime di truffe? Denunciare alle Autorità e chiedere rimborso**

Se doveste essere vittime di truffe di questo tipo, potete sporgere denuncia presso le autorità e avvisare immediatamente Poste Italiane del raggiro subito. E' un vostro diritto chiedere il rimborso alle Poste Italiane S.p.A. per le eventuali somme che vi sono state fraudolentemente sottratte dal truffatore. E' la stessa Corte di Cassazione ad avere affermato che spetta all'istituto di credito (Banca o Poste Italiane) verificare la riconducibilità delle operazioni effettuate tramite*home banking* alla volontà del cliente, impiegando la diligenza dell' "accorto banchiere" e che in mancanza il correntista debba essere risarcito (*Ordinanza n. 9158 del 12 aprile 2018*).

# SHOPPING ONLINE, CONSIGLI PER L'USO

Gli acquisti in rete possono far risparmiare, ma devono essere eseguiti in tutta sicurezza, soprattutto per quello che riguarda i dati delle carte di credito. Ecco, se stai leggendo questo articolo, significa che hai bisogno di qualche consiglio su dove acquistare in rete, cosa vale la pena comprare, gli shops virtuali, trucchi per evitare le truffe, metodi per pagare in sicurezza ed evitare così inutili delusioni. Internet offre una serie infinita di possibilità, con l'esplosione dell'e-commerce, infatti, è possibile acquistare su internet qualsiasi tipo di prodotto e servizio, comodamente da casa, dall'auto (ferma), in bicicletta (ferma) o su una panchina al parco. Permette talvolta di risparmiare soldi e qualche volta di fare affari. Si può riuscire a trovare un assortimento e una varietà di prodotti impareggiabili e in tempi molto rapidi. Anche nel mondo degli acquisti in rete, però, ci sono rischi, truffe e brutte sorprese. Conosciamo bene questa nuova realtà dello shopping! Per comprare su internet è dunque necessario conoscere e imparare le regole e i diritti dell'acquirente. Bisogna sempre ragionare sul prezzo, il vero risparmio va fatto sommando al prezzo di ciò che comprate le spese accessorie (quindi imballo e spedizione), e il totale deve giustificare l'acquisto in termini di risparmio rispetto al negozio tradizionale. Le spese di spedizione dipendono dal peso del pacco. L'acquisto su internet conviene più per oggetti piccoli e di valore elevato, che per oggetti di grandi dimensioni e/o pesanti, ma caratterizzati da prezzo medio o addirittura basso. Altro elemento importante è l'assistenza, ossia garanzia e manutenzione. Occorre quindi avere tutte le garanzie e l'indicazione dei centri di assistenza, dove potersi recare per una eventuale riparazione o altre necessità.


Può accadere, infatti, di acquistare in Germania un cellulare, per poi scoprire che non viene riparato in Italia. Da verificare anche la qualità dei prodotti venduti che viene garantita dal venditore. La spedizione, quando si compra in internet, è un aspetto da non trascurare, poiché al prezzo reale dell'articolo andranno sommate le spese di spedizione che dipendono, oltre che dalle caratteristiche dell'articolo, anche dalle stesse modalità di spedizione. Molti siti di negozi virtuali indicano con chiarezza l'ammontare delle spese di spedizione, altri no e il prezzo diventa una incognita. Talvolta le spese accessorie sono nascoste e solo dopo aver effettuato l'acquisto veniamo a conoscenza del reale ammontare. Prima di acquistare occorre, quindi, verificare sempre il costo della spedizione e chiarire se vengono realmente fatte spedizioni ove risiedete. Inoltre l'acquistare da paesi stranieri extra Europa impone le pratiche per lo sdoganamento, con il relativo obbligo di pagare il dazio di importazione e l'IVA . LA MERCE ORDINATA È PROPRIO QUELLA? Non potendo vedere il prodotto dal vivo, ci potrebbe essere la spiacevole sorpresa di ricevere un oggetto che non corrisponde a quanto da noi ordinato, considerato che i modelli sono tanti e le differenze sostanziali. Tra l'altro, gli acquisti su internet talvolta sono preceduti da una visita al Centro Commerciale per avere un'idea sulla merce, a causa di questa prassi alcuni negozi si sono stancati di fare le vetrine fisiche, per poi favorire gli acquisti su internet a prezzi inferiori senza il rincaro dovuto alle spese per pagare affitto e dipendenti.

Cosicchè alcuni negozi hanno avanzatola richiesta di un costo per provare ad esempio un paio di scarpe. Ci sono settori, come in particolare quello dell'abbigliamento e dei prodotti alimentari di marca, dove è facile che vengano messe in vendita su internet delle imitazioni e delle contraffazioni, magari perfette. Come tutti sanno il falso*made in Italy*è diffuso ormai ovunque. Più il venditore è grande e conosciuto, maggiori sono le garanzie che offre. Acquistare in rete da negozi online con magazzino in Italia è sempre fonte di garanzie maggiori che non comprare all'estero via internet.

## L'angolo dei tuoi diritti

Per la legge italiana chi acquista fuori dai locali italiani ha sempre il diritto di recesso basta che lo faccia valere entro un termine ben preciso: 14 giorni dall'acquisto, come da decreto legislativo 206/2005 art. 52. Se hai qualche dubbio o vuoi chiedere dei chiarimenti contatta il venditore, per telefono o via e-mail, consulta qualche forum per vedere se altri consumatori hanno lasciato opinioni o giudizi sul venditore. Stampa la pagina del sito: se per qualche ragione la transazione si dovesse interrompere e non sei certo dell'esito, inviala tramite raccomandata al venditore. Non utilizzare la carta di credito su computer pubblici.

## Tutte le informazioni sul sito per gli acquisti online

Verifica sempre: le caratteristiche del prodotto; il prezzo (comprensivo di IVA); le spese di spedizione; che sia indicato il nome del venditore (persona fisica o Società) con i recapiti fisici (indirizzo recapito telefonico) per poterlo contattare in caso di problemi. La partita IVA, se registrata presso la Camera di Commercio; le modalità di pagamento e di consegna e il relativo termine che non deve superare i 30 giorni;

che l'indirizzo del sito inizi con*https*e ci sia il logo del lucchetto; che siano indicate le condizioni e la procedura del diritto del recesso (il reso), se dovessero mancare queste indicazioni, ricorda che il termine per esercitarlo si allunga , per legge a 12 mesi e 14 giorni.

## I consigli della polizia di stato

La Polizia Postale ha elaborato una serie di consigli utili per guidare in tutta sicurezza sia chi inizia solo ora a fare acquisti online sia gli habituè dell'e-commerce, che, comodamente da casa propria, con pochi click, possono fare shopping evitando spiacevoli sorprese.

## Marketplace

I siti commerce marketplace (come Ebay) pubblicano sulle loro pagine online annunci di altri venditori, privati o negozi fisici. In questi casi le condizioni contrattuali che si applicano all'acquisto sono quelle del venditore, mentre Eprice obbliga i venditori alle proprie condizioni. Tramite i servizi della rete internet si può anche comprare direttamente da privati da tutto il mondo, infatti, a migliaia mettono in vendita oggetti e prodotti di ogni tipo, sia nuovi che usati, sui siti di aste on line, il più celebre dei quali è Ebay. Quest'ultimo non è ovviamente l'unico nel suo genere ma di certo risulta essere il più longevo e il più affermato. I siti di aste offrono agli utenti iscritti (mediante semplice registrazione e attribuzione di ID e Password) la possibilità di vendere e acquistare ogni genere di oggetto. Il loro sistema di gestione degli utenti iscritti prevede un'ampia gamma di regole e di meccanismi filtro per aumentare e garantire la tutela di venditori ed acquirenti. Questi sistemi sono peraltro in continuo aggiornamento. Nonostante tutto ciò, bisogna sempre tenere gli occhi aperti e valutare molto bene quel che si va a comprare, ma, soprattutto, da chi si compra. Smanettando su Ebay andate sempre a vedere il feedback del venditore e cercate così di capire a chi ha venduto in precedenza, cosa ha venduto e quel che dicono di lui gli altri utenti.

# MARMELLATE FATTE IN CASA, SOS BOTULINO!

L'inverno si avvicina ed è il momento giusto per mettersi all'opera e preparare conserve di frutta. Scegliere le materie prime di buona qualità è sicuramente un buon punto di partenza per avere un prodotto genuino, ma occorre anche seguire le procedure corrette per evitare rischi.

## Che cos'è il botulino?

Il botulino è un microrganismo che si trova nel suolo, vive in assenza di ossigeno. Il batterio può produrre diverse tossine, alcune delle quali sono responsabili del botulismo. Si tratta di una malattia paralizzante che, a seconda della dose di tossina ingerita, può avere diversi livelli di gravità. È necessario prestare molta attenzione, soprattutto riguardo le conserve domestiche, che sono le più soggette al pericolo di botulino. Prima di indicarvi le linee guida per una conserva senza rischio occorre approfondire alcuni aspetti.

Ecco i sintomi:

I primi sintomi compaiono generalmente tra le 12 e le 36 ore successive all'assunzione di cibo contaminato: si può avvertire debolezza, avere vertigini o sensazioni di paralisi. Possono comparire altri sintomi come vomito, difficoltà respiratorie, diarrea etc. Nelle prime ore della comparsa dei sintomi è possibile curare l'intossicazione con una terapia specifica. In quali cibi si può sviluppare la tossina? La tossina responsabile del botulismo può trovarsi nelle conserve preparate male, ad esempio nelle conserve di frutta e verdura preparate in casa. La causa scatenante potrebbe essere il non aver rispettato correttamente certe procedure. Nei cibi commerciali è raro che si possa sviluppare la tossina, a meno che i barattoli non siano danneggiati.

Vademecum

**Igiene personale e della cucina.**

La prima fonte di contaminazione può essere rappresentata proprio da due fattori, l'igiene personale e della cucina.Presta attenzione all'igiene in ogni fase della lavorazione, per evitare la presenza del batterio fin dall'inizio.

**Attrezzature.**

Per la preparazione delle conserve sono necessari diversi utensili comunemente disponibili in una cucina domestica. Il vetro è il materiale migliore, anche se possono essere utilizzati contenitori in metallo. Scelta degli ingredienti. Per ottenere conserve di frutta e verdura che mantengono intatti i sapori, gli aromi e le fragranze delle materie prime, è ideale scegliere sempre prodotti di stagione, perché più ricchi di sali minerali, vitamine, e nutrienti.Seziona accuratamente le materie prime.

**Lavaggio dei prodotti.**

Lavare le materie prime sotto acqua corrente in modo da eliminare le particelle di terra ed altri eventuali residui. L'immersione per qualche minuto in acqua contenete il bicarbonato di sodio può essere utile per ridurre tracce di pesticidi dalla superficie esterna dei vegetali.

**Sterilizzazione dei contenitori.**

Il termine sterilizzazione si riferisce a un trattamento in grado di distruggere tutte le forme microbiche, comprese le spore.

**Riempimento dei contenitori.**

I contenitori non vanno mai riempiti fino all'orlo, ma è necessario lasciare uno spazio vuoto indispensabile affinché all'interno del contenitore si generi il vuoto, inoltre, serve per contenere l'aumento del volume della conserva durante il trattamento termico.Non riempire i contenitori fino all'orlo, è necessario il cosiddetto "spazio di testa" perché si generi il vuoto. Pastorizzazione delle conserve: L'unico trattamento di stabilizzazione termica possibile in ambiente domestico è la pastorizzazione. Si fa immergendo completamente i contenitori in acqua. Coprire la pentola con il coperchio e portare l'acqua ad ebollizione. A questo punto l'erogazione del calore può essere regolata a livello più basso, ma comunque in grado di garantire sempre un ebollizione uniforme e vigorosa.Finita la preparazione, i contenitori devono bollire per almeno 10 minuti: le alte temperature distruggono le tossine.

**Verifica dei contenitori :**Dopo la pastorizzazione, il contenuto dei vasetti sarà visibilmente diminuito a causa dell'estrazione dell'aria. Trascorse 12-24 ore, quando i contenitori saranno ben raffreddati, devono essere accuratamente ispezionati per valutare l'ermeticità della chiusura e il raggiungimento del vuoto. I tappi o capsule di metallo dovranno apparire leggermente concavi (incurvati verso l'interno del contenitore).

**Evita di riutilizzare gli stessi tappi.**

Dopo aver seguito attentamente le nostre linee guida potrai preparare un'ottima conserva di frutta o verdura!

# IL LIBRO È UN BENE ESSENZIALE. BOOKCITY MILANO NON SI FERMA.

**Le librerie aperte: il libro come bene essenziale.**

La fase buia che stiamo attraversando, a causa dell'emergenza sanitaria, ci porta a riflettere sull'importanza del libro e della lettura. Il libro, dunque, è un bene essenziale. Il nuovo Dpcm, in tal proposito, tra le tipologie di commercio al dettaglio che possono rimanere aperte anche nelle zone rosse, ha incluso le librerie.

**La lettura produce benefici.**

La lettura è un'attività potenzialmente molto ricca di benefici, a breve e a lungo termine, per la salute psicologica e per la salute in generale. Oltre a migliorare le competenze linguistiche, logiche e di comprensione del testo, aiuta ad ampliare le proprie capacità critiche, la conoscenza di se e degli altri e la conoscenza del mondo in generale.

**La lettura al tempo del Coronavirus**

Così come affermato da Paolo Ambrosini (presidente dell'Associazione Librai Italiani), e da Riccardo Franco Levi (presidente dell'Associazione Italiana Editori), "i libri sono beni essenziali e, soprattutto in un momento come questo, possono aiutare gli italiani a superare la solitudine e le difficoltà legate alle limitazioni della libera circolazione e della socialità."


**L'iniziativa bookcity**

Su questa linea d'onda si muove Bookcity Milano, che rimane aperta e non si ferma. Bookcity Milano ha l'obiettivo di mettere al centro di una serie di eventi diffusi sul territorio urbano il libro, la lettura e i lettori, come motori e protagonisti dell'identità della città e delle sue trasformazioni nella storia passata, presente e futura. L'iniziativa è stata voluta dal Comune di Milano e dall'associazione BookCity Milano.

**Il programma di bookcity**

Anche quest'anno Bookcity Milano ha presentato il suo programma per il periodo compreso tra l'11 novembre e il 15 novembre. Si tratta di eventi online che toccano diversi temi della lettura che vanno dalla *narrativa* alla *storia* e all'*attualità*, da *musica* e *spettacolo* al *tempo libero*. Un tema particolare che mira a valorizzare la cultura della città di Milano e a raccontare la storia di chi l'ha fatta grande: "*Milano racconta Milano*".

# ABBONAMENTO

# 2020

## € 60,00

LEGGI SU TELEFONO O TABLET
(ANDROID/APPLE)

**CLICCA QUI**