RISPARMIO & FUTURO

Papillon o mascherina ?

... questo è il dilemma!

Sede Nazionale ADUSBEF, via Bachelet n. 12, p. 1° - 00185 - ROMA

Mensile anno XXXII– N°12 - 1° Dicembre 2020

Sped. in abb. Postale DL 353/2003 (Conv. in L. 27/02/2004 n° 46) art. 1 comma 1 DCB Roma

RISPARMIO & FUTURO prodotto e distribuito da ADUSBEF APS ETS

TRASPARENZA INFORMAZIONE CERTEZZA DEL DIRITTO NELLA CONTRATTAZIONE

Anno XXXII – N° 12- **Dicembre 2020**

Periodico d'informazione
Direttore Responsabile Elio Lannutti
Amministrazione, Redazione e Stampa: Via Bachelet n. 12, 00185 ROMA
Autorizzazione del Tribunale di Roma N° 299 del 18 maggio 1988
Abbonamenti: Ordinario € 25 euro; Sostenitore € 100 e oltre.
Versamenti su **conto corrente postale** IBAN: IT74S0760103200000070043005 oppure su **conto corrente bancario** presso Monte dei Paschi di Siena IBAN: IT35Q 01030 03204 000001471949, sempre intestato ad Adusbef.
Redazione: Antonio Tanza - Fabio Massimo Blasi - Mauro Novelli – Federico Novelli - Giuditta Satriano – Alessandra - Rosalba Di Placido - Donato Surano - Salvatore Ruberti - Mario Fasano - Stella Vera De Benedittis - Emanuela Mollona - Giuseppe Palamà - Tania Saracino - Patrizia Rossetti - Luisa Frassanito - Filomena Cosentino - Olga Tanza.
Corrispondenti: Daniele Imbò (LE); Vincenzo Laudadio (BA); Giuseppe Angiuli (BA); Orazio Isidoro Scuro (BA); Angela Dell'Aquila (BR); Paola Licia Follieri (FG); Raffaele Rutigliano (FG); Giuseppe Sbriglio (AO); Lucia Monacis (TO); Anna Patisso; (TO) Daniele Folino (VB); Andrea Sella (BI); Giovanni Piazza (MI); Caterina La Sala (MI);Fulvio Cavallari (PD); Sveva Rossi (PD);Manuela Spada (RO); Monica Spada (Vi);Emanuela Marsan (VI); Camilla Cusumano (VR); Emanuela Bellini (VR); Paola Formica (MC); Daniela Rossi (AP); Paolo Polato (TN); Federico Capalozza (UD); Patrizia Monferrino (GE); Anna Maria Patisso (GE); Alessandra Malatto (GE); Silvio Boccalatte (GE); Grazia Angelucci (BO); Alberto Basaglia (RA); Giulio Caselli (FI); Andrea De Cesaris (GR); Fabrizio Mirko (LU); Andrea Frosini (PO); Floro Bisello (PU); Silvia Surano (PG); Riccardo Falocco (TR); Alessandra Di Sarno (RM); Fiammetta Fiammeri (RM); Massimo Campanella (RM); Giuliano Forlani (RM); Maria Elena Catelli (FR); Carlo delle Site (RM); Angelo Turriziani (RM); Antonio Serafini (Rm); Veronica Mattei (RM); Maria Rita Di Giambattista (PE); Doriana Pescara (CB); Monica Cirillo (NA); Ivan Lambiasi (SA) Maria Teresa De Bottis (CE); Vittoria Marzioni (PZ); Felice Belisario (PZ); Elena Mancuso (CZ); Lucia Cittadino (CZ); Fernando Scarpelli (CS); Angela Blando (PA); Giorgio Panzeca (PA); Elisabetta Freni (CT); Marianna Orlando (ME); Nicola Marchese (ME); Serena Lazzaro (SR); Gaspare Di Maria (AG); Guenda Pili (CA); Alberto Marongiu (OR); Antonino Siffu (SS); Elisabetta Cristiani (MI); Cristiano Aretusi (TE); Antonio Stagnaro (GE).

Sommario del n° 12 – Dicembre 2020

Note a margine dei convegni organizzati dal progetto "***e-RA DIGITALE***".

On line e sistemi di pagamento elettronici: la loro debolezza strutturale dipende anche da noi...

(Un pretesto anche per evidenziare alcune curiosità)

di Mauro e Federico Novelli

Sommario

1) Truffe on line e con sistemi di pagamento elettronici.

A cura del MEF (Direzione V Ufficio VI) l' UCAMP – Ufficio centrale Antifrode dei mezzi di pagamento - edita annualmente un *"Rapporto statistico sulle frodi con le carte di pagamento"*. Col ruolo di supporto e consulenza dell'UCAMP opera il GIPAF (Gruppo di Lavoro Interdisciplinare per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento) di cui fanno parte ABI, Bankitalia, Poste, esponenti bancari, forze di polizia e tre membri indicati dal CNCU ed altri operatori di settore. Nel 2011 il CNCU indicò, quali membri esperti, Francesco Avallone - Federconsumatori, Fabio Picciolini – Adisconsum e Mauro Novelli - Adusbef. Il Gipaf ha funzioni consultive.
L'ultimo Rapporto (n° 9 del 2019) relativo all'anno 2018, relaziona di dati particolarmente interessanti circa le frodi tramite carte di pagamento distinte per canali di utilizzo.
Tratta dal 9° Rapporto, riportiamo una tavola riepilogativa:

Illuminanti i dati relativi al canale Internet.
Nel 2018, il 74% del valore delle frodi ha utilizzato Internet come canale. Di minore frequenza sia il canale POS (17%) che quello del Bancomat (9%).
Il dato più preoccupante è fornito dal numero relativo di euro frodati sul totale del valore delle operazioni effettuate con carte di pagamento: mentre ogni 100.000 euro 4 sono frodati via POS e 2 via ATM, sul canale Internet sono frodati 2,2 euro su 1.000 (mille) euro. Complessivamente, sono frodati 1,12 euro su 10.000 euro trattati.
Quanto al numero delle operazioni effettuate on line, sono frodate 0,94 operazioni ogni 10.000.
Stiamo parlando di rilevazioni del 2018. A parte la normale evoluzione intervenuta nel 2019, desta preoccupazione il fatto che con la pandemia da coronavirus e la necessità/decisione di uscire molto meno da casa, molti concittadini hanno deciso di affrontare il mondo degli acquisti on-line, dell' e-commerce, dei pagamenti con moneta elettronica ecc. Questi concittadini sono stati spinti dalla situazione pandemica ad adottare i nuovi strumenti

informatici obtorto collo, pur non essendo molto esperti e ancor meno entusiasti. Ci auguriamo che i futuri Rapporti UCAMP per il 2020 ed anni successivi non facciano emergere una situazione disastrosa circa le frodi perpetrate nel settore.
Il Rapporto Ucamp n°7 del 2017 ci permette alcune comparazioni tra i dati 2018 e quelli del 2016. Notiamo alcuni buoni miglioramenti:

Tra le altre comparazioni possibili:
· Nel 2016 il 55% del valore delle frodi ha preso decisamente la strada di Internet (74% nel 2018).
· Nel 2016 ben 3 euro su 1.000 sono stati frodati via internet, contro i 2,2 euro del 2018.
· Nel 2016 sui tre canali (Internet, Pos, ATM) 1,64 euro sono stati frodati ogni 10.000, contro 1,12 euro del 2018
· Nel 2016 complessivamente 1,29 operazioni su 10.000 sono state frodate, contro lo 0,94 del 2018
Possiamo quindi affermare che, tra il 2016 ed il 2018, i presidi di sicurezza sono migliorati e che le frodi si vanno accumulando sul canale Internet, alleggerendo notevolmente i POS e gli ATM.

2) Non rifiutiamo le nuove tecnologie: piuttosto conosciamole meglio e organizziamoci allo scopo utilizzarle per un vero progresso dell'umanità .
Nel corso dell'ultimo convegno organizzato nell'ambito del progetto e-RA DIGITALE abbiamo appreso che società criminali, esperte di informatica, sono in grado di violare tutto, di copiare tutto, di sostituirsi a tutti. Ciò vuol dire che dobbiamo "gettare in mondezzaro" le nuove tecnologie? Certo, se consideriamo "normale" ed immutabile l'attuale stato dell'arte sarebbe opportuno accantonare tutto. Ma dobbiamo considerare che siamo solo all'inizio dell'era digitale. Tale ambiente iniziale ha permesso alle organizzazioni più svelte e senza scrupoli (quelle criminali) di operare in un mercato brado, non libero, senza leggi. Quindi in mercato non regolato. Si sa che le azioni di contrasto poste in essere dalla società civile sono lente e macchinose, ma – pur se con lentezza – prima o poi torneranno ad imporre le condizioni perché il mercato torni ad essere "libero".
Questo stato di cose, lungi dallo scoraggiarci, deve imporci uno sforzo intellettuale (personale e sociale) perché le nuove tecnologie informatiche non cadano completamente in mano a cyber criminali e, anzi, ad essi siano sottratte. Se si procedesse ad organizzare convegni sui pericoli che affronta chi cammina in strada, scopriremmo che, nel periodo 2015-2016, l'ISTAT stima che il 6,2 % dei cittadini ha subito borseggi, scippi, aggressioni e rapine, mentre il 5% dei cittadini ha subito truffe informatiche e clonazione delle carte bancarie.
Insomma, tutti abbiamo assunto – più o meno frequentemente - una medicina che ha queste controindicazioni: angioedema, ulcera peptica, anamnesi positiva per sanguinamenti intestinali, colite ulcerosa, morbo di Crohn o storia pregressa per le stesse patologie, sanguinamento cerebrovascolare, diatesi emorragica o concomitante terapia anticoagulante, insufficienza renale, insufficienza epatica, asma, ipofosfatemia ed infezioni virali. Ma non per questo siamo propensi a smettere l'utilizzo dell'Aspirina.
Occorre rendersi conto che l'utilizzo dei nuovi strumenti è stato convulso e brado, ed ha avuto la enorme comodità quale catalizzatore per far breccia nel

consumatore quindi non regolato dal legislatore che, solo da pochi anni, si affanna ad aggiornare la normativa esistente, ritenendo che questa potesse applicarsi fruttuosamente anche alle ICT. Questo ritardo (legislativo, fiscale, finanziario ecc.) ha permesso la nascita e la crescita di enormi oligopoli che travalicano frontiere, lingue, comunità e reti finanziarie. Ha permesso la nascita e lo sviluppo di criminali informatici in grado di violare qualsiasi presidio di sicurezza.
Nella fase che stiamo attraversando, all'eterna e obbligata rincorsa tra aggressore e difensore, si stanno sommando le inadeguatezze legislative a quelle di impreparazione e approssimazione in termini di conoscenze tecniche personali. Ma mentre alla ineludibile rincorsa tra offesa e difesa non possiamo porre fine, possiamo ben porre fine ai ritardi legislativi, fiscali, di presidi di sicurezza – e della tendenza a non investire molto in essi, lasciando che se la sbrighino gli utenti - di conoscenza tecnica personale e del conseguente uso pressappochistico delle tecnologie. Insomma, non possiamo rinunciare alle scoperte della metallurgia perché da esse sono nate le spade occorre riflettere sul fatto che la metallurgia ha permesso di produrre anche aratri.
E' necessario quindi operare su più fronti. In campo socio politico occorrerà creare gruppi di studio, capaci farsi gruppi di convinzione/pressione, perché il legislatore adotti nuove norme finalmente adeguate, imponga migliori presidi di sicurezza, anche contrattuali (si pensi ai contratti di conto corrente bancario. Si veda oltre), riveda completamente la materia senza sperare nella funzionalità di norme periodicamente rabberciate in fretta, ma create quando non esistevano neanche le fotocopiatrici.

3) Curiosità. Alcune novità e qualche proposta.
Società criminali sono in grado di ottenere duplicati e sostituzioni di Sim e carte di credito; di inserirsi nel tragitto informatico seguito da operazioni on line; di mettere fuori gioco cellulari (Sim) quando vogliono. E' ineludibile, quindi, che i presidi di sicurezza debbano essere progettati e costruiti sul terreno internazionale e della collaborazione tra stati; su quello legislativo nazionale, attraverso un ripensamento complessivo ed intelligente della materia da normare; sul fronte contrattuale in grado di imporre investimenti adeguati alle aziende che offrono servizi bancari e finanziari; nel campo personale attraverso una educazione, a partire obbligatoriamente dalla scuola, per mettere in grado tutti i cittadini di acquisire correttamente rudimenti di informatica e di conoscere, con metodo, i pericoli dell'uso criminale delle nuove tecnologie.
Sul versante delle istituzioni internazionali, si è assistito ad una afonia generalizzata in grado di rendere muti i grandi organismi mondiali e i grandi stati in grado di incidere sulle caratteristiche delle ICT. Questo ha lasciato il campo libero alla formazione di oligopoli potentissimi in grado ormai di condizionare la vita di miliardi di cittadini. Ha lasciato altresì il campo libero a che si traslasse il "battere moneta" nel campo merceologico: le cripto valute, le valute non cripto (in Italia il Sardex è tra le più consolidate) , entrambe comunque complanari alle monete battute dalle zecche dei vari stati, sono prodotte e trattate come una merce qualsiasi, con vantaggi tali per quanti intendono operare nell'ombra, da far loro trascurare il problema della fiducia che da sempre deve accompagnare una moneta perché sia accettata dal mercato. Gli stessi giganti del web si stanno cimentando nel battere moneta. Facebook sta ritardando il lancio della sua valuta virtuale (la Libra) perché dal "consorzio" di gestione si sono tirate via sia Mastercard che Visa, con molta probabilità per la reazione dei sistemi bancari che potrebbero aver minacciato il boicottaggio dei loro servizi.

Quanto alle piattaforme di e-commerce, altro campo ormai dominato dagli oligopoli, Google potrebbe presto inserire delle funzionalità nuove nella sua piattaforma video Youtube. Attraverso queste funzionalità, tramite il conosciutissimo contenitore si potrebbero fare acquisti. Già oggi sono presenti sul portale numerosi youtubers e influencer che recensiscono prodotti di vario tipo (telefonini, dispositivi elettronici, elettrodomestici, capi d' abbigliamento...). Gli influencer spesso inseriscono, all' interno dei loro interventi dei link o dei coupon per l'acquisto dei prodotti recensiti. Presto potrebbe esserci un salto di qualità: Youtube chiederebbe ai creatori di contenuti (cioè coloro che fanno i video) di taggare e monitorare i prodotti che recensiscono; attraverso i tag, Google fornirebbe poi ai potenziali compratori i link diretti all' acquisto su una piattaforma commerciale propria. Il salto di qualità finale potrebbe essere proprio questo: fare transazioni commerciali direttamente su Youtube. Del resto l' e-commerce sui social network è già una realtà grazie ai Facebook Shops e agli Instagram Shops. E presto, quindi, potremmo addirittura fare shopping direttamente attraverso Whatsapp.
Questi nuovi strumenti di acquisto, sicuramente molto comodi per i consumatori, al tempo stesso nascondono numerose insidie (in tema di privacy e possibili truffe) che queste nuove frontiere degli scambi commerciali portano con sé.
Di fronte a questo pervasiva attività dei nuovi oligopolisti, il settore bancario e finanziario internazionale (e i potentati che si è costruito a supporto) è stato motivato a reagire nel momento in cui quegli oligopoli hanno inteso invadere il settore della finanza e, parallelamente, il settore delle criptovalute conquistava anche la fiducia dei cittadini venendo benevolmente accolto da molti operatori che non vedevano l'ora di potersi scaricare di dosso il giogo mondiale della finanza ufficiale.
Come sempre, sono i banchieri i più capaci e svelti nell'impostare nuovi sbocchi ai propri affari e agli interessi di settore. [Si pensi all'introduzione dell'euro, fortemente voluta proprio dalla finanza europea, quando ancora i paesi della UE si esercitavano a questionare tra di loro su tutto. Abitudini che non hanno perso]. Per non essere sopravanzati e travolti dal nuovo stato di cose, hanno ripensato velocemente i loro "prodotti industriali", aggiornandoli.
Comunque, c'è da osservare che i costi del cyber crimine sono molto alti e non conviene ai malintenzionati prendere di mira conti o patrimoni non "capienti" o considerati poco interessanti. Anche questa valutazione potrebbe entrare nei calcoli di rischiosità dei sistemi informatici architettati. Oltretutto, non conviene ai cyber criminali inflazionare il loro sistema di commissione del reato per asciugare i conti di scarso i9nteresse finanziario.

3.1) L'euro digitale.

Il 2 ottobre 2020 la BCE ha pubblicato un rapporto sulla possibile introduzione di un euro digitale [https://www.ecb.europa.eu/euro/html/digitaleuro.en.html]. In essa viene esaminata l'emissione di una valuta digitale della banca centrale (CBDC), l'euro digitale, dal punto di vista dell'Eurosistema. Un simile euro digitale – si legge - può essere inteso come moneta della banca centrale offerta in forma digitale per essere utilizzata da cittadini e imprese per i pagamenti al dettaglio. Completerebbe l'attuale offerta di contanti e depositi all'ingrosso delle banche centrali. Ne parlano due banchieri: Christine Lagarde: "gli europei stanno ricorrendo sempre di più a soluzioni digitali per pagare, risparmiare e investire. Dato che il nostro ruolo è garantire la fiducia nella moneta unica, questo significa accertarsi che l'euro sia adatto all'era digitale. Quindi dobbiamo essere preparati a emettere l'euro digitale, se dovesse presentarsene la necessità". A queste fanno anche coro le parole di Fabio Panetta, membro del Comitato esecutivo

della Bce che nei giorni scorsi è intervenuto proprio in merito alla possibilità di creare un euro digitale verso la metà del 2021, sottolinea come: "l'immobilismo non è un opzione". "La tecnologia e l'innovazione stanno cambiando il modo in cui consumiamo, lavoriamo e interagiamo con gli altri", spiega Panetta. "L'introduzione di un euro digitale sosterrebbe la spinta dell'Europa verso la continua innovazione, contribuendo inoltre alla sua sovranità finanziaria e al rafforzamento del ruolo internazionale dell'euro", conclude il banchiere centrale.
Ci si augura che la sicurezza operativa dell'euro digitale sia all'altezza della situazione, non potendosi la BCE permettere di fallire (troppo facilmente) sotto i colpi dei nuovi criminali.
Probabilmente adotterà tutti quegli strumenti, anche molto costosi, che gli istituti bancari e le finanziarie tendono a tralasciare lasciando al cliente poco protetto il compito di correre dietro al problema di truffa, di furto di identità ecc.

3.2) Adeguare la legislazione nazionale in materia.
Nel corso del convegno e-RA DIGITALE tenutosi a Pesaro, al Questore Pineschi veniva chiesto se banche e finanziarie avessero la possibilità di verificare se i documenti di identità presentati, ad esempio per aprire conti, fossero di libera detenzione, magari consultando le banche dati delle forze dell'ordine. Il Questore Pineschi informava che banche e finanziarie (non so se anche le Camere di commercio) non possono – se non in rarissimi casi – interrogare le banche dati dei documenti smarriti o rubati. Poiché, quindi, quegli elenchi non sono accessibili, chi si presenta in banca per aprire un conto può impunemente presentare quei documenti senza che l'istituto di credito possa verificarne la regolare circolazione. Mi raccontava un amico avvocato che con i documenti smarriti da una sua zia sono state aperte società.
Nella fattispecie, occorre pressare il legislatore perché renda non solo possibile, ma addirittura obbligatoria per banche, finanziarie, Camere di commercio ecc. la consultazione degli elenchi dei documenti di identità smarriti o rubati, detenuti da CC, Polizia, Guardia di Finanza ecc. Le entità interessate potrebbero creare, presso ogni filiale di città (quindi non in tutte le agenzie) un ufficio accreditato collegato con le forze dell'ordine per interrogare, anche non in via diretta, le banche dati di cui si parla.
Abbiamo scritto alla Crif ed alla filiale di Roma della Banca d'Italia perché valutino la possibilità di istituire d'iniziativa una loro banca dati di documenti d'identità rubati o smarriti (certamente su base volontaria) affinché chi subisce il furto o smarrisce documenti di identità possa chiedere di inserire i riferimenti nei loro elenchi. Con questa iniziativa si cerca di contrastare il furto di identità, evitare a banche e finanziarie potenziali truffe e raggiri, salvaguardando in tal modo anche il cittadino colpito dalla vicenda.

3.3) Modificare i contratti e gli articoli che riguardano la gestione on line dei conti correnti, del Bancomat, delle carte di credito.
Sarebbe opportuno procedere ad una modifica di alcuni contratti bancari. Ad esempio quelli relativi al Bancomat e alle carte di credito dovrebbero prevedere che alcuni dati finanziariamente sensibili (come i massimali di prelievo giornalieri e mensili) siano modificabili esclusivamente per via cartacea dal cliente, con raccomandata o raccomandata a mano consegnata agli sportelli, di cui il cliente conserverà copia. Sta poi alla banca adottare adeguati sistemi di sicurezza per la loro protezione perché il cyber criminale non sia in grado di violarli tanto facilmente. Certamente la soluzione non risolve il problema, ma ha lo scopo di richiamare l'attenzione del cliente sulla gravità delle sue scelte, potenzialmente foriere di guai e di spingere le banche ad adottare migliori sistemi di sicurezza. Si fa

presente che in molti casi la sottoscrizione dei contratti di cui si tratta viene effettuata senza informare adeguatamente il cliente sui massimali di alcune voci "sensibili": il cliente dovrebbe poter essere chiamato a decidere se effettuare o impedire bonifici all'estero, il limite massimo dei suoi bonifici, dei suoi assegni, oltre che dei massimali su Bancomat e carte. Deve altresì poter decidere se l'eventuale modifica di quelle voci vada effettuata per raccomandata. Certamente per il cliente si tratta di un impaccio che, però, oltre a renderlo consapevole della gravità delle decisioni, potrebbe evitare molte tristezze successive.
Si ricorda che una ventina di anni fa, in occasione della necessità di tradurre in euro i valori in lire dei contratti bancari, si sono verificati casi in cui alcune banche, di iniziativa, aumentarono i massimali su prelievi bancomat senza avvertire il cliente: "Sa, quei massimali erano troppo bassi… l'abbiamo fatto nel suo interesse…"

Da www.adusbef.it Il CONSIGLIO. Massimali Bancomat: sorpresa! Di Mauro Novelli 22-11-2001

Quando richiedemmo la carta Bancomat/PagoBancomat, firmammo un contratto e definimmo gli importi massimi prelevabili giornalmente e mensilmente come POS o, in contan dagli sportelli automatici (in genere, 500.000 lire giornaliere - 258,23 euro- con un massimo di 3.000.000 di lire mensili - 1549,37 euro).Con la motivazione di favorire il client molte banche hanno aumentato tali massimali senza nulla comunicare al titolare della carta. Alcuni correntisti hanno scoperto di avere massimali giornalieri pari a 10 milioni di lir 5.164,57 euro), dopo aver subito furti (prelievi e pagamenti illeciti) per svariati milioni nello stesso giorno. "Ma come, io posso prelevare solo 500 mila lire al giorno, mentre truffatore può farlo per svariati milioni !?!?!"Guardi, lei non lo sa, ma per favorirla abbiamo aumentato il suo massimale ....." Riprendete il contratto Bancomat/PagoBancomat a suo tempo firmato: - verificate i massimali indicati.- scrivete una Raccomandata A.R. alla Presidenza della Banca (per conoscenza alla Banca d'Ital per conoscenza a noi [indirizzi alla voce Banche e Clienti dell'Indice del sito]) nella quale ribadite che quel massimale contrattuale è ancora in vigore, che ne vieta tassativamente il superamento e che in caso di trasgressione riterrete responsabile degli ammanchi la banca. Se non siete in possesso del contratto, richiedetene una copia vostro sportello.(MN)

3.4) *Avast secure browser.* **Indicazione attendibile**?

Nel corso di un confronto telefonico con l'Ispettore Filippelli della Polizia Postale di Catanzaro, si chiedeva un parere sul browser realizzato da Avast. La nota società produttrice dell'omonimo antivirus dichiara che nella versione "banca", estensione attivabile dal suo browser, "i dati sono al sicuro".
La "certificazione" appare sulla destra della barra in basso non appena si attiva la modalità banca (vedi foto). Poiché, come sostiene l'Ispettore Filippelli, tutto è informaticamente violabile, quella certificazione di sicurezza lascia molto perplessi. Comunque potrebbe essere oggetto di verifica (ingannevolezza?) da parte dell'Antitrust.
Ecco la dizione in basso a destra della videata di Avast secure browser in modalità "banca".

3.5) Lo skimmer non va in pensione.

Lo skimmer è una geniale soluzione criminale per entrare in possesso dei codici relativi ad un Bancomat o ad una carta di credito. L' aggeggio è un lettore di bande magnetiche e ripropone la fessura dell'ATM dove viene introdotto e sistemato. Il cliente che inserisce la carta per effettuare un'operazione non sa che, prima della macchina, i suoi codici sono letti e registrati dallo skimmer. Il criminale, ritirato dalla fessura il marchingegno elettronico di sua proprietà, potrà poi, in tutta tranquillità, leggere e riprodurre su altra tessera i riferimenti del cliente. Con quella tessera potrà a ritirare i contanti.
Con lo skimmer, alcuni anni fa, sono stati fatti molti danni. Oggi non va più di moda perché i cittadini sono stati adeguatamente, ma c'è sempre la possibilità che il detentore possa entrare in possesso dei codici segreti semplicemente inserendo nel suo apparecchietto tenuto in casa (e non pensionato) la carta rubata o rinvenuta da un complice.
Questo spiega come mai, in molte circostanze, il ladro abbia potuto ritirare contanti ancor prima che il malcapitato si accorga del furto e proceda al blocco della carta. Non è vero, come asseriscono banche e gestori di moneta elettronica, che il furto è stato possibile perché il titolare della tessera, venendo meno all'obbligo contrattuale di conservare adeguatamente

i codici segreti, ha appuntato il pin ed ha conservato l'appunto assieme alla carta mettendo il ladro in grado di prelevare agevolmente. Basta che il criminale abbia un complice dotato di skimmer per entrare in possesso dei dati e poter prelevare contanti.

3.6) Quando fui assunto in banca …

(un lontano ricordo di Mauro Novelli)

Alleggeriamo il discorso!

Entrai in banca – assunto a Padova nel 1974 - per un corso di qualificazione postuniversitario di un anno (così erano allora denominati i master).

Fui affidato ad un funzionario prossimo alla pensione per formalizzare la mia posizione (apertura del conto ecc.).

Prese i moduli da firmare e…: " Questi sono i tre moduli che i clienti devono firmare quando aprono un conto. Anche tu depositerai la firma per la sottoscrizione dei tuoi ordini alla banca: si chiamano "spèsimen".

Ragionai sul termine per un attimo.

Gli feci presente che forse si trattava di latino e non di inglese, dunque si sarebbero dovuti chiamare "specìmen" con l'accento sulla i. Non insistetti perché capii che era rimasto male. Comunque firmai gli spèsimen. Mi chiese, poi, di avere la mia Carta di identità. La osservò, ma prima ancora di registrarla sugli spèsimen, mi fece osservare con atteggiamento protettivo che sarebbe stato molto pericoloso depositare in banca la stessa firma da me usata per tutte le sottoscrizioni, dalla richiesta del certificato di residenza alla sottoscrizione di un abbonamento ad un periodico, al deposito della firma sul documento di identità. Riconobbi che aveva ragione. Dopo essermi esercitato con una firma diversa, gli chiesi di risottoscrivere gli spèsimen. Da allora la mia firma in banca (oggi in Poste) è diversa da quella che appongo in qualsiasi altra circostanza.

Ho adottato il metodo dell'univocità dei riferimenti da fornire alla banca anche per quanto riguarda il numero di cellulare e l'indirizzo di posta elettronica. Il mio conto ha un numero di cellulare ed un indirizzo di posta elettronica dedicati ed esclusivi.

La Sim di quel cellulare costa (PosteMobile) due euro al mese, la e-mail è invece gratuita. Il sistema non risolve il problema del furto di dati o di identità, ma comunque non mi creano ansia: se arrivano messaggi *"bancari"* equivoci sul mio numero di cellulare pubblico o sul mio indirizzo e-mail comunicato a tutti, so che sono tentativi truffaldini.

Se invece il messaggio equivoco mi arriva sul numero di cellulare o sulla posta elettronica forniti alla banca o alla Posta, so che o hanno violato gli archivi detenuti da quelle aziende o che si è alla presenza di impiegati infedeli che si son rivenduti i miei dati.

Violazione dei presidi di sicurezza. Possibilità e probabilità. Dieci punti da approfondire.

di Mauro e Federico Novelli

Col procedere degli approfondimenti esplicitati nel corso dei convegni organizzati nell'ambito del progetto e-RA DIGITALE sulle truffe on line e sul cyber crimine, gli interventi degli addetti ai lavori (Alfonso Scarano, Francesco Zorzi, Francesco Cocchi ed altri) ci stanno ponendo di fronte ad una situazione drammatica: chi ha valenze finanziarie on line come conti correnti, carte di credito ecc. non si salverà. In altri termini, le capacità dei cyber criminali sono tali e le loro conoscenze informatiche sono talmente profonde e professionali da metterli in grado di violare qualsiasi presidio di sicurezza, sia esso organizzato da banche, finanziarie, fiduciarie ecc. Quindi ad ogni correntista non resta che attendere il suo turno per lo svuotamento

di qualsivoglia contenitore dei suoi capitali.
Ma se le cose stessero in maniera granitica come descritte, ad una associazione di utenti non resterebbe che impostare una massiccia campagna informativa rivolta ai clienti bancari perché rinuncino all'operatività on line dei loro rapporti con le banche, per tornare alla più tranquilla gestione dei propri affari bancari, fatta con interventi di persona, "su strada". Stessa azione dovrebbe essere intrapresa da coloro che operano nel campo della sicurezza dei sistemi informativi: se sono convinti che i criminali possono tutto e non ci sono ostacoli per loro insormontabili, dovrebbero altrettanto chiaramente e pressantemente convincere i cittadini ad abbandonare le gestioni finanziarie on line.
Poi però, sempre i nostri esperti ci informano che il sistema bancario non adotta alcuni presidi di sicurezza di buon livello perché troppo costosi (lasciando al malcapitato cliente di correre personalmente dietro alle truffe) e che dovrebbe crearsi un gruppo di pressione perché le banche siano obbligate ad investire per migliorare i loro sistemi di salvaguardia dei correntisti che operano on line.
Queste considerazioni cambiano radicalmente le carte in tavola. Il discorso sulla sicurezza da assoluto diventa immediatamente relativo: da "ogni presidio è superabile dai criminali onnipotenti" (possibilità di violare), a "esistono presidi più difficilmente violabili dai criminali" (probabilità di violare).
Viene così recuperato anche il ruolo delle associazioni di consumatori attraverso informazioni, consigli, raccomandazioni ai propri associati ed ai correntisti in genere.
Eccone alcune.

1) Smettiamola con la ricerca affannosa della velocità, della semplicità e della comodità di esecuzione, **soprattutto nel campo delle operazioni finanziarie on line.**
Abbandonare il mito della velocità, della semplicità e della comodità di esecuzione degli obbiettivi che vogliamo raggiungere. Più il sistema ci permette di raggiungerli facilmente e senza passaggi "rognosi", più è possibile che ci renda intrappolabili da parte della rete cybercriminale, per via del grande numero di dati sensibili che dobbiamo affidare ad altri. Questo meccanismo compulsivo fa premio sulla sicurezza delle operazioni.

2) Usare smartphone che abbiano il riconoscimento tramite impronte digitali.
Dagli interventi dei nostri esperti ci sembra di aver capito che se le app di gestione di un conto corrente on line sono attivabili tramite impronta digitale il sistema di sicurezza risulta meno facilmente violabile rispetto a quello che richiede solo la PW. A detta di tutti, invece, non è assolutamente affidabile il riconoscimento facciale, tanto che i costruttori di smartphone inseriscono questo warning direttamente tra le istruzioni del telefonino. Abbiamo quindi individuato una prima barriera più difficilmente scavalcabile. Quindi premere perché si usino smartphone che abbiano il riconoscimento dell'impronta digitale.

3) Il fenomeno della "sim swap" si elimina cancellando la possibilità di ottenere duplicati delle Sim originali.
Alcuni siti di gestori finanziari raccomandano di non diffondere ai quattro venti il proprio numero di cellulare, perché, in genere, tale numero è anche quello utilizzato quale ulteriore livello di sicurezza attraverso la gestione degli OTP autorizzativi. La raccomandazione è fornita perché se si è titolari di una Sim e questa, oltre a permetterci telefonate, sms e collegamenti in rete, viene accreditata per l'autorizzazione di operazioni sul conto corrente, è facile per il criminale procedere ad intrusioni di successo

sostituendo una sua sim clonata a quella originale.
Ma tenere riservato il numero di cellulare è un ossimoro! Abbiamo personalmente attivato da tempo una Sim (2 euro al mese) dedicata unicamente alla funzione di gestione autorizzativa di operazioni sul C/C tramite la ricezione di OTP. Quel numero è conosciuto solo da noi e dal gestore di telefonia, a meno che il cyber criminale non abbia valenze aperte con qualche impiegato infedele del gestore telefonico o sia stato in grado di violarne gli archivi informatici. Trattandosi di sim non operativa per l'uso normale (mai usata per telefonare, mai usata per accedere al web), la mia è stata relegata su un vecchio Nokia di sedici anni fa. Questo cellulare non ha l'operatività in rete: credo risulti difficile al criminale procedere alla clonazione ed alla sua esclusione (se non tramite l'azione di un dipendente infedele del mio gestore di telefonia) per sostituirsi nella ricezione delle comunicazioni autorizzative. Comunque le truffe tramite "sim swap" possono essere tagliate alla radice vietando ai gestori di telefonia la possibilità assoluta di effettuare duplicati di sim rubate, smarrite o danneggiate. Il cambiamento della sim di regolamento del conto e delle carte dovrà essere effettuato personalmente recandosi in agenzia o in ufficio postale.

4) In subordine, obbligate almeno l'operatore telefonico a fare una telefonata al numero di cui il criminale richiede il duplicato.
In attesa che si riesca ad imporre il divieto di duplicazione delle Sim, i gestori di telefonia impongano agli operatori, ai quali il criminale chiede il duplicato della Sim, di rimandare di 24 ore l'emissione della nuova Sim duplicata, e di effettuare, nel frattempo, una serie di tentativi di contattare per telefono il numero indicato come non più utilizzabile (per smarrimento, furto, distruzione dello smartphone). Potrebbe scoprire subito che quella Sim è viva e vegeta.

5) Resettare a fondo gli apparecchi (magari vecchiotti) destinati a gestire le nostre finanze.
Per le operazioni finanziarie on line non usare un device dove i ragazzi hanno scaricato centinaia di giochi e tanta paccottiglia pericolosa. Soprattutto non usare lo stesso computer per l'operatività on line dei vari conti della famiglia.

6) Per l' e-commerce usare una carta prepagata.
Le spese di e-commerce vanno gestite non tramite il conto corrente, ma tramite una carta prepagata dove terremo giacenti pochi euro. Con le prepagate le spese on line sono gestibili anche in assenza di conti correnti o in presenza di conti correnti che non abbiano la gestibilità on line. La ricaricheremo in funzione degli acquisti on line programmati, effettuati i quali, il saldo tornerà ad essere di pochi euro: in caso di violazione cyber criminale, il danno sarà di piccola entità. Oltre che tramite app, le ricariche dal conto corrente possono essere effettuate tramite ATM, quindi approfittando dei sistemi di sicurezza delle banche, di Poste, delle finanziarie.
Se siamo inclini all'esterofilia, possiamo anche attivare prepagate radicate in altri paesi. La N26 è ad esempio tedesca, con società di gestione a Francoforte, quindi con iban teutonico.

7) Adusbef prema per la modifica dei contratti sottostanti al sistema on line.

Più che con iniziative individuali del correntista miranti a porre dei paletti al sistema ed all'ente che gestisce il suo conto corrente, è opportuno che Adusbef ponga in essere una azione mirante a fare pressioni d'impatto ma "ragionate" presso il legislatore e le autorità monetarie e di controllo affinché vengano modificati i contratti sottoscritti dal cliente. Nei contratti per la gestione on line del conto, occorrerebbe imporre modifiche che forniscano al consumatore la possibilità di

definire quali servizi e operazioni possano essere modificati accedendo direttamente al sistema informatico e quali quelli modificabili unicamente col classico strumento della raccomandata con AR o "a mano" consegnata allo sportello (facendosi firmare una copia per ricevuta).
Del resto, già il contratto di delega sul C/C, che autorizza un terzo ad operare sul conto, permette al correntista di decidere quali operazioni sono consentite al delegato e quali no. Ad esempio il titolare può decidere di permettere al delegato la firma degli assegni, ma non di poterne ritirare il libretto allo sportello. Da decenni è offerta al correntista questa possibilità in materia di delega, e l'informatizzazione dei servizi bancari ha tenuto conto di quelle opzioni.
Allo stesso modo, il correntista deve poter decidere quali operazioni "bloccare" (con possibilità di modificarle solo per raccomandata) da una lista di operatività che il contratto deve elencare esplicitamente. Il sistema deve adeguare obbligatoriamente i suoi processi informatici perché sia in grado di gestire queste nuove opzioni senza la necessità di interventi umani.
Pensiamo con fondatezza che azioni individuali miranti ad ottenere gli stessi risultati non avranno successo. E' da ritenere che la banca non accetterà quelle integrazioni contrattuali apportate da clienti isolati se dovesse valutare (o decidere) che il rispetto dei vincoli imposti da un singolo correntista risulti troppo costoso e troppo oneroso dal punto di vista procedurale e dei controlli da porre in essere: le banche non amano le eccezioni procedurali, rifuggono da gestioni personalizzate che scantonino eccessivamente dalla gestione informatica processata in automatismo ed obblighino a costosi - e fallibili - interventi umani. E siccome la banca non è obbligata e tenere come cliente me, Persichetti (o Agnelli, si diceva qualche decennio fa), convocherà il correntista e cercherà di convincerlo a ritirare blocchi e cancelletti. Se non riesce nell'operazione di convincimento, gli metterà a disposizione le somme da lui detenute in banca e procederà alla chiusura del conto (soprattutto se parliamo di Novelli e non di Agnelli).
Quella della pressione per la modifica generalizzata dei contratti è la strada che suggeriamo ad Adusbef, assieme ad imporre il divieto di duplicare le Sim. La nostra associazione dovrebbe farsi capofila per creare un movimento con tali scopi: se saremo capaci di raggiungere l'obbiettivo i cambiamenti apporteranno benefici alle stesse banche.
Suggeriamo di pianificare un'azione ben coordinata anche alla luce delle novità che potrebbero ben presto intervenire nell'operatività della BCE che ha in progetto la creazione di un euro digitale e, quindi, di valenze dirette della banca centrale con i cittadini di Eurolandia attraverso la creazione di conti in moneta unica digitale. Questa iniziativa non può fallire troppo facilmente sotto i colpi dei cybercriminali e, per renderla di successo, le autorità di Francoforte decideranno di destinare tutti gli investimenti necessari affinché sia garantito il massimo di sicurezza informatica al sistema ed ai cittadini futuri correntisti di BCE. Questo atteggiamento, parallelo alla nostra azione, potrebbe essere preso ad esempio da tutti i sistemi bancari della UE, rendendoli più propensi a spendere per la loro sicurezza e per quella dei correntisti. Non è oltretutto escluso che la BCE metta a disposizione del sistema bancario di Eurolandia i punti di forza dei suoi sistemi di protezione.

8) Stiliamo noi un articolato dei contratti più diffusi e sottoscritti in banca, di conto corrente e contratti accessori, di custodia titoli ecc. Li sottoporremo quindi al sistema bancario per vedere l'effetto che fa.

Potrebbe essere utile recuperare una vecchia iniziativa proposta ad Adusbef ma che non ha avuto mai seguito: stiliamo noi un articolato di contratto per conto corrente, custodia titoli ed altri; togliamo ogni clausola vessatoria; inseriamo la

normazione di argomenti nuovi non contemplati dai vecchi contratti (come quelli trattati in questa sede) e sottoponiamoli agli istituti di credito. Potrebbero avere successo, quanto meno per motivi di concorrenza.

9) Oltre il progetto, predisponiamo documentazione per i consumatori, anche video, di esplicitazione dei problemi e delle soluzioni individuate.

Dal lato dell'utente/consumatore, invece, le associazioni dei consumatori dovrebbero proseguire e intensificare al massimo i momenti e gli strumenti di informazione, formazione e sensibilizzazione. Fare cultura e diffondere la conoscenza degli argomenti che hanno un impatto sulla vita quotidiana dei cittadini deve essere una delle missioni delle associazioni. Pertanto, sulla base di quanto l'ADUSBEF sta facendo con il progetto e-RA DIGITALE - IL CONSUMATORE INCONTRA IL WEB e, in particolare, con i seminari che si stanno svolgendo in questi ultimi mesi, si potrebbe proseguire – oltre il progetto - l' azione di diffusione di cultura e conoscenza per realizzare una vera educazione consumeristica; ciò può essere fatto continuando ad approfondire l'argomento con i seminari e archiviandoli sul sito in modo che possano essere resi fruibili, magari attraverso un contributo economico oppure ai soli iscritti; in più, si potrebbero produrre dei video non eccessivamente lunghi, divisi per tematica, nei quali gli esperti danno informazioni e consigli. Questi video – extra progetto - potrebbero essere visionabili e fruibili solo per gli iscritti all' associazione.

10) Sicurezza delle operazioni on-line: la concorrenza tra sistemi bancari è mondiale.

Nell'e-commerce, nella gestione delle finanze personali e familiari on line e in generale nella finanza on line la concorrenza travalica i confini nazionali.

Se sistemi bancari di altri paesi si doteranno di sistemi di sicurezza dell'operatività on line manifestamente superiori a quelli nostrani, sarà molto facile accedere ad essi. Il metodo più semplice di passare a gestioni estere è quello di diventare titolari di carte di credito prepagate non radicate in Italia, quindi con Iban estero. Siccome abbiamo pagato tutte le tasse dovute sui redditi in Italia, il loro utilizzo è del tutto legittimo. Basta dichiararne la titolarità.

Dott. Mauro Novelli

Dott. Federico Novelli (Consulente Adusbef)

PROCESSO EX PROMOTORE FINANZIARIO DI IW BANK S.p.a.
ADUSBEF PARTE CIVILE

Il tribunale di Terni autorizza anche la chiamata in causa del responsabile civile .

(IL GATTO E LA VOLTE NON DORMONO MAI - PARTE I)

Prosegue innanzi al Tribunale di Terni in composizione monocratica, il procedimento che vede coinvolto un promotore finanziario ternano, accusato di truffa con l'aggravante dell'aver cagionato alla persona offesa un danno di rilevante gravità. e di cui la prima udienza si è celebrata il 15 giugno 2020 (R&F numero n. 7 del 1 Luglio 2020).

Alla prima udienza il Tribunale di Terni nella persona del giudice Dott.ssa Fratini, ha ammesso quale parte civile nel processo, l'Associazione di consumatori Adusbef, difesa dall'Avv. Massimo Campanella del foro di Roma, trattandosi di associazione specializzata nella tutela dei clienti del sistema bancario, promuovendo per statuto, la tutela dei fondamentali diritti alla correttezza, trasparenza ed equità nella costituzione e nello svolgimento dei rapporti contrattuali concernenti beni e servizi, con particolare riguardo ai servizi finanziari e creditizi (v. L. 7 marzo 1996 n.108).

Alla successiva udienza, celebratasi, il 9 novembre 2020, il Tribunale di Terni, ha accolto la richiesta della difesa dell'imputato, di riunione del procedimento con altri già pendenti a carico dell'imputato, inoltre sulle richieste della difesa di Adusbef per la chiamata in giudizio del Responsabile Civile il Giudice ha ordinato, per tale ragione, la chiamata in causa della IW Bank s.p.s., fissando udienza per il giorno 01.02.2021, al fine di verificare la comparizione in giudizio del Responsabile Civile e di discutere in ordine al richiesto patteggiamento dell'imputato.

Si vuole qui in breve ricordare la vicenda.

L'imputato, ex promotore finanziario della IW Bank S.p.a., in seguito a numerosi reclami presentati da clienti, ha subìto dalla Consob, a novembre 2018, una sospensione cautelare, dall'esercizio dell'attività di consulente finanziario abilitato all'offerta fuori sede, per il periodo di sessanta giorni. Le contestazioni riguardavano: violazioni concernenti la consegna di rendicontazioni false, contenenti una situazione finanziaria maggiore rispetto a quella reale, o una movimentazione non autorizzata, o la falsificazione della firma su modulistica contrattuale o l'ammanco di somme. Al termine del periodo di sospensione il promotore veniva radiato.

L'ammissione quale parte civile di Adusbef, nel processo di Terni dello scorso 15 Giugno, è solo l'ultima in ordine di tempo, infatti sin dalla sua nascita l'Associazione ha sempre tutelato i risparmiatori costituendosi nei processi dove erano coinvolti promotori finanziari e banche. La rassegna stampa sarebbe molto lunga, cito solo alcuni di tali procedimenti.

Nel 2014 il Tribunale di Taranto ha condannato Banca MPS per l'operato di un suo promotore finanziario, e nel 2016 il caso di un promotore finanziario bergamasco accusato di aver truffato risparmiatori del varesino e della provincia di Lecco, con 100 querele ricevute ed un portafoglio in gestione per oltre 24 milioni di euro.

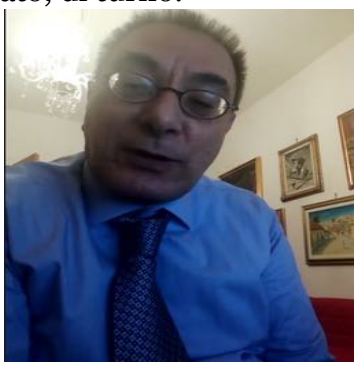
Sicuramente per la vicinanza con il luogo dove si è celebrato il recente processo di Terni, vale la pena di rammentare la sentenza del 2017 della Corte di Appello di Perugia, che ha condannato la Banca Mediolanum al risarcimento dei danni per l'attività illecita del promotore finanziario

In breve si vuole ricordare quali siano gli obblighi di un promotore finanziario.

E' un professionista (agente o dipendente), abilitato alla promozione e al collocamento presso i clienti di servizi finanziari e prodotti di investimento proposti dalla banca, società di intermediazione mobiliare (SIM) o società di gestione del risparmio (SGR) per cui lavora.

Pertanto consiglia il cliente, suggerisce gli strumenti finanziari più adatti e assiste il risparmiatore nella scelta degli

investimenti (titoli azionari, obbligazioni, fondi comuni di investimento, prodotti per la gestione del risparmio, polizze vita), ma è vincolato a proporre solo i prodotti e i servizi della propria società.
Per questa sua attività viene poi remunerato dalla banca o dalla società, con una retribuzione variabile in base ai contratti conclusi.
Il lavoro del promotore finanziario consiste nel contattare e incontrare i clienti, attuali o potenziali, per vendere i servizi e gli strumenti finanziari, attraverso un colloquio, comprende e analizza le necessità finanziarie dei clienti: ne valuta la situazione economica, le esigenze di risparmio e investimento, le aspettative e la propensione al rischio, in base a queste informazioni è in grado di proporre soluzioni finanziarie adeguate agli interessi dei clienti, scegliendo tra i servizi e prodotti emessi dall'istituto per cui lavora, inoltre il promotore finanziario deve informare sulla natura dell'investimento e sui potenziali rischi, illustrare i vantaggi del prodotto offerto e rispondere a tutte le domande in maniera chiara ed esaustiva, affinché il cliente possa effettuare scelte consapevoli.
Il promotore finanziario ha infatti l'obbligo deontologico di tutelare gli interessi del risparmiatore e di garantire trasparenza e correttezza nell'esercizio della propria attività. Il promotore finanziario raccoglie il denaro per conto dei clienti e lo colloca nei prodotti di investimento scelti, secondo gli accordi stabiliti dal contratto, inoltre deve assicurarsi che la documentazione necessaria per effettuare l'investimento venga sottoscritta da entrambe le parti, l'intermediario e il cliente.
Dal lato deve crearsi un rapporto di fiducia tra cliente e promotore finanziario, dall'altro vi è un obbligo deontologico del promotore finanziario di tutelare gli interessi del clienti, ed il denaro raccolto per conto dei clienti deve essere collocato nei prodotti scelti.
Più in generale con questo breve articolo si vuole porre l'attenzione degli utenti-consumatori-investitori, sulle possibili truffe finanziarie che possono avvenire per il tramite di una gestione truffaldina dei risparmi, come nei casi summenzionati, o con le nuove frontiere delle truffe, realizzate ad esempio sul trading on-line da broker senza scrupoli (e di cui tratterò in un prossimo articolo).
" I vari modi di interagire con i clienti da parte di fornitori di servizi di investimento truffaldini, possono essere particolarmente insidiosi, proprio perché l'operatore tende a disorientare il risparmiatore cercando di stringere con lui anche un rapporto personale", aggiungerei anche per conoscere il reale stato patrimoniale del soggetto e quello familiare.
E' proprio il caso di ricordare la favola di Pinocchio di Collodi, ed i personaggi del Gatto e la Volpe i truffatori per eccellenza, quelli capaci di irretire a tal punto l'ingenuo ed impreparato Pinocchio da convincerlo a sotterrare le sue monete nel Campo dei Miracoli, dove sarebbe cresciuto un albero pieno di Zecchini d'Oro che lo avrebbe fatto diventare ricco.
Oggi il Gatto e la Volpe hanno nomi diversi, spesso sono legati alla tecnologia, hanno estensioni e ramificazioni in tutto il mondo e sono loro, moderni Gatto e la Volpe a raccontare la favola sempre moderna (e sempre da ricordare) del Campo dei Miracoli, che esisterà sempre per fare sparire le monete del Pinocchio, malcapitato, di turno.



Avv. Massimo Campanella
(Componente del Direttivo Nazionale

La redazione ed i corrispondenti di ***Risparmio & Futuro*** *augurano ai loro lettori ed agli associati* **ADUSBEF** ***Buona Salute*** *e*

BUONE FESTE !

TRAPARENZA, INFORMAZIONE e CERTEZZA DEL DIRITTO NELLA CONTRATTAZIONE

ASSOCIAZIONE DI PROMOZIONE SOCIALE (APS) -ENTE DEL TERZO SETTORE (ETS)

DAL MAGGIO 1987, ADUSBEF APS ETS COMBATTE ASPRE BATTAGLIE IN DIFESA DEI DIRITTI DEI CITTADINI IN OGNI SETTORE CONSUMERISTA ED È PARTICOLARMENTE SPECIALIZZATO IN CREDITO, FINANZA E ASSICURAZIONI.

FINALITA' DELL'ASSOCIAZIONE: in termini culturali e di bagaglio tecnico, Adusbef Aps Ets è attrezzata per operare con peculiare incisività nei settori: bancario, finanziario, assicurativo, postale, delle telecomunicazioni, della giustizia

RAPPORTO CON GLI ASSOCIATI: le nostre iniziative sono elaborate partendo sempre dalla realtà dei fatti, e diffuse tramite il periodico "Risparmio & Futuro" e attraverso comunicati stampa. Gli Associati coinvolgono l'Adusbef informando su argomenti dallo sviluppo manifestatamente non corretto o sospetto, richiedendo direttamente consulenze o semplici risposte a quesiti, coinvolgendo l'associazione su problemi di utenza e di consumo.

STRUTTURA. SEDI: Oltre la sede nazionale romana di via Vittorio Bachelet n. 12 Adusbef Aps Ets conta oggi più di 190 sedi locali ed è presente in tutte le Regioni d'Italia.

I professionisti responsabili delle delegazioni in cui si articola l'Associazione, sono in maggioranza avvocati. Tutti hanno sottoscritto il codice etico, elaborato originariamente nel dicembre 2000, il cui testo si può reperire sul nostro sito (www.adusbef.it) dove sono presenti tutte le sedi ufficiali Adusbef.

SE VUOI AIUTARCI A CONTINUARE LE NOSTRE BATTAGLIE IN DIFESA DEI TUOI DIRITTI…..
….. ISCRIVITI ALL'ADUSBEF Aps Ets

Socio ordinario (validità biennale)	**- 25 euro (12,50 euro per anno)**
Socio ordinario (validità annuale)	**- 12,50 euro**
Socio ordinario simpatizzante (validità biennale)	**- 5 euro (2,50 euro per anno)**
Socio ordinario simpatizzante (validità annuale)	**- 2,5 euro**
Socio ordinario sostenitore (validità annuale)	**- 100 euro e oltre**

- VERSAMENTI SU CONTO CORRENTE **POSTE ITALIANE**
  IBAN: IT74S0760103200000070043005 INTESTATO ADUSBEF;
- OPPURE SU CONTO CORRENTE BANCARIO PRESSO **MONTE DEI PASCHI DI SIENA SPA**
  IBAN: IT35Q0103003204000001471949 INTESTATO ADUSBEF;
- OPPURE ISCRIVITI **ONLINE**: https://web.adusbef.it/iscrizione_socio.asp
- OPPURE ISCRIVITI PRESSO LA DELEGAZIONE ADUSBEF (https://www.adusbef.it/sedi);

CI DARAI UNA MANO A BATTERE LA PREPOTENZA DI UN POTERE POLITICO FINANZIARIO SEMPRE PIÙ SUPPONENTE ED ARROGANTE CHE MORTIFICA PERFINO QUEI DIRITTI ACQUISITI ED INALIENABILI DEI CITTADINI E DEI CONSUMATORI IN TUTTI I CAMPI. GRAZIE DELL'ATTENZIONE.

Finanziamenti pubblici ricevuti da Adusbef nell'anno 2019: importo: **€ 7.896,92** Erogato da: MISE per il tramite di Movimento Consumatori – Io sono originale anno 2017-2018; importo: **€ 3.392,06** Erogato da: da MISE per il tramite di Movimento Consumatori- Terra dei fuochi; importo: **€ 600,00** Erogato da: da MISE per il tramite di Movimento Consumatori – Caccia al tesoro; importo: **€ 71.162,06** Erogato da: da MISE per il tramite di Movimento Consumatori – Io sono Originale; importo: **€ 17.210,00** Erogato da: Regione Lazio per il tramite di Federconsumatori Lazio – Map 7; importo: **€ 65.164,91** Erogato da: Mise per il tramite di Federconsumatori Nazionale – progetto Er@ Digitale; Importo: **€ 13.012,59** Erogato da: Cinque per Mille - Oggetto: erogazione Quote Cinque Per Mille Anno 2017 2016; Importo: **€ 36.533,65** Erogato da: Presidenza Del Consiglio dei Ministri Mef CONTRIBUTOASSOC.CONSUMATORI D.LGS 70.2017 Editoria ANNO RIF. CONTR. 2018.

*"Per difendere meglio i tuoi diritti destina il **5 per mille** delle tue imposte a sostegno di **Adusbef**. Indica il codice fiscale della nostra associazione **0 3 6 3 8 8 8 1 0 0 7** sul modulo della denuncia dei redditi ed apponi la tua firma."*