REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ILLEGALITA', CONTRAFFAZIONE E ABUSIVISMO

LE GUIDE PER LA TUTELA DI PROSSIMITA' DEL CONSUMATORE

II

Le truffe sul web

A cura della ATS La Tutela di Prossimità del consumatore

Materiale informativo predisposto e realizzato nell'ambito del Programma generale di intervento della Regione Sardegna con l'utilizzo dei fondi del Ministero dello sviluppo economico. Ripartizione 2018

Prefazione

Un consumatore informato è un consumatore consapevole ed è in grado di fare scelte responsabili. Con questa finalità abbiamo realizzato le Guide per "La tutela di prossimità del consumatore".

Questa guida nasce da una domanda molto semplice.

Ci siamo chiesti come poter aiutare concretamente i nostri consumatori anche quando questi non avranno la possibilità o il tempo di contattarci subito per domandarci una risposta ai propri dubbi.

Ed allora ci siamo concentrati sull'esigenza di affiancare alla nostra presenza capillare sul territorio alcune azioni concrete che permettano al consumatore di essere sempre più consapevole e preparato.

Siamo convinti che la nostra azione debba passare anche attraverso una garanzia di tutela "a distanza" in un'ottica di informazione e formazione continua che ci renda tutti più forti.

La tutela di prossimità è anche questo: vi saremo vicini i nostri consigli anche quando non avrete il tempo di contattarci!

Noi tutti, infatti, non sempre facciamo scelte razionali. Che si tratti dell'offerta più conveniente al supermercato, della scelta del tasso del mutuo, del confronto fra le condizioni di assicurazione o della scelta del regime alimentare da seguire, si rischia continuamente di fare scelte poco convenienti per la mancanza di informazioni sufficienti.

La nostra esperienza sul campo, però, ci permette di fornirvi alcune informazioni partendo dall'esame delle situazioni portate alla nostra attenzione e degli errori più prevedibili per aiutarvi a porvi le domande giuste e a scegliere in modo meno istintivo nelle materie più rilevanti (alimentazione, salute, educazione, risparmio, pensione), senza privarvi della possibilità di scegliere consapevolmente.

*Questa modalità di intervento correttivo del percorso decisionale individuale è stata chiamata da alcuni studiosi "**architettura delle scelte"** ed il nostro scopo, nel nostro piccolo, è proprio quello di creare in ogni lettore la struttura delle alternative rilevanti.*

Solo in questo modo saremo più forti ed influenti e riusciremo a tutelarci!

Abbiamo deciso di dedicare la seconda guida al tema delle truffe sul web perché ormai una gran parte delle transazioni si svolge su un "territorio virtuale" nel quale si trovano giorno dopo giorno le maggiori insidie.

Buona lettura!

Avv. Federica Deplano – Presidente Movimento Difesa del Cittadino di Cagliari

Giorgio Vargiu – Presidente Adiconsum Sardegna

Giorgio Vidili – Presidente Cittadinanzattiva Sardegna

GLI ACQUISTI E LE TRANSAZIONI SUL WEB – UNA REALTA' IN FREQUENTE CRESCITA

Quanti di noi decidono di acquistare un qualunque oggetto usato su internet ed utilizzano i più noti portali nati negli ultimi anni per questa finalità?

Sembra sempre estremamente facile: una cifra modesta per acquistare un qualunque prodotto, magari pubblicizzato come mai utilizzato e messo in vendita da una affidabile signora a cui è stato regalato e che ha deciso di non utilizzarlo e, quindi, di venderlo ad un prezzo molto conveniente. La comunicazione avviene tramite *e-mail* o via *whatsapp*; ci viene fornita anche la copia di un documento di identità e i dati per il trasferimento di denaro mediante una ricarica.

La venditrice, fino al momento del pagamento, è gentilissima ed attenta a chiarire ogni dubbio.

Salvo, poi, sparire dopo l'avvenuto pagamento senza naturalmente consegnare l'oggetto venduto.

Le modalità ormai sono le più disparate, ma la storia è sempre la stessa.

Da una velocissima ricerca che ognuno di noi potrà compiere, emergerà subito la portata e la mole di operazioni che singoli, associazioni dei consumatori, forze dell'ordine e legali conducono nei confronti di centinaia di vittime, la cui unica colpa è stata quella di essersi fidati un po' troppo.

Ci fidiamo un po' troppo anche quando utilizziamo i portali di pagamento in maniera disincantata e quando involontariamente forniamo i dati dei nostri conti correnti. Dati che dovremmo custodire gelosamente ma che, senza renderci conto, forniamo in vario modo a soggetti terzi.

Ci sono casi in cui fra due interlocutori che stanno dialogando a distanza via email si frappone un terzo soggetto che assume l'identità di uno di essi ed intrattiene con l'ignaro interlocutore rapporti per acquisire informazioni riservate al fine di porre in essere bonifici e pagamenti vari.

In altri casi, vi è invece un furto massivo di identità digitali attraverso email varie che inducono la vittima a rilasciare direttamente le proprie informazioni personali (username, password e informazioni personali).

L'obiettivo di queste truffe informatiche è fare incetta di dati personali e, quindi, estorcere con l'inganno dei soldi.

Per prevenire le situazioni sopra descritte e, in particolare, per non incorrere nel rischio di inviare denaro a qualcuno che non ci consegnerà mai nessun bene per poi sparire nel nulla, dobbiamo ricordarci in primo luogo che vi è quasi sempre uno schema tipo:

- L'acquirente, interessato soprattutto dal prezzo conveniente, instaura una comunicazione, il più delle volte tramite *email*, col presunto venditore che tende a veicolare la transazione trasmettendo grande affidabilità e serietà;
- Il venditore, per non destare sospetti, fornisce copie di documenti di identità ed anche un numero di cellulare, del quale non è mai l'intestatario: se contattato telefonicamente, risponderà prontamente fino all'avvenuto pagamento, per poi rendersi irreperibile. Solitamente tali numeri, intestati a prestanome consenzienti o a inconsapevoli cittadini,

sono utilizzati per un certo numero di truffe e poi sono disattivati: per truffe successive saranno intestate nuove SIM;

- Lo stesso venditore spinge l'acquirente a concludere la trattativa evitando l'incontro di persona. Le scuse addotte possono essere le più varie: in genere, dopo una iniziale disponibilità incondizionata ad uno "scambio a mano", lo stesso farà apparire l'impossibilità dell'incontro di persona, e la conseguente conclusione a distanza, come una ineluttabile conseguenza;
- Successivamente chiede come forma di pagamento il metodo che offre minori sicurezze e garanzie per l'acquirente: ovvero la ricarica di carte prepagate, sperando che il malcapitato non conosca la carenza di tutela di tali forme di pagamento;
- L'acquirente, quindi, procede al pagamento ma non riceverà mai ciò che ha acquistato;
- Il truffatore, dopo aver ricevuto il pagamento, non si farà mai più sentire né si intimorirà per il ricevimento di minacce di denuncia o segnalazioni alla Polizia Postale.

Dunque, la prima regola è l'attenzione a queste modalità di azione.

Accertatevi sempre di poter effettuare il pagamento contestualmente alla consegna della merce o che, comunque, ci sia di fronte a noi un soggetto affidabile. L'attenzione non è mai troppa.

LA SOTTRAZIONE DEI DATI DEI NOSTRI STRUMENTI DI PAGAMENTO

Quanto alla seconda tipologia di truffe, ovvero quelle che implicano la comunicazione dei nostri dati e l'utilizzo degli stessi online, possiamo imparare e mettere in pratica alcune importanti regole che ci permetteranno quanto meno di diminuire la probabilità di avere problemi.

Eccole riassunte di seguito.

Utilizzare sempre e solo software sicuri

Curare costantemente gli aggiornamenti sul proprio computer

Il primo passo per operare online in tutta sicurezza è avere sempre un sistema operativo ed un buon antivirus aggiornati all'ultima versione. Questo comportamento ci consente di avere sempre protezione nella fase della scelta degli acquisti su Internet. Per una maggiore sicurezza, inoltre, è necessario aggiornare all'ultima versione disponibile il browser utilizzato per navigare, poiché le possibili minacce sono in continua evoluzione.

Navigare sempre su siti sicuri e verificare che lo siano prima di effettuare l'acquisto.

Non avere fretta e darsi sempre il tempo di verificare la sicurezza dell'operazione

Al momento di ogni acquisto dobbiamo verificare la sicurezza del sito: assicurarsi sempre che la pagina web su cui si sta effettuando il pagamento sia contrassegnata dalla presenza di un lucchetto, caratterizzata dall'estensione "*https*" anziché "*http*", visualizzabile nella barra degli indirizzi del browser di navigazione. Questi elementi indicano la presenza di un canale sicuro ed affidabile. Inoltre, prima di completare qualsiasi tipo di acquisto, è buona norma verificare che il sito prescelto sia fornito di riferimenti quali un numero di Partiva IVA, un numero di telefono fisso, un indirizzo fisico e ulteriori dati per contattare l'azienda: un sito senza tali dati probabilmente non è affidabile.

Occhio al ribasso!

Su internet è possibile trovare ottime occasioni, ma quando un'offerta si presenta troppo conveniente rispetto all'effettivo prezzo di mercato del prodotto che si intende acquistare, allora è opportuno procedere ad una verifica su altri siti: potremmo trovarci di fronte a un falso o a una truffa.

Leggere sempre i commenti e le recensioni

Internet oggi ci da un vantaggio: chi ha avuto esperienze negative ha la possibilità di dare molto risalto a ciò che è capitato mediante le recensioni. Leggetele sempre! Si trovano sul sito dell'oggetto messo in vendita, oppure su siti esterni, motori di ricerca, forum o social. Anche le

informazioni sull'attendibilità del sito tramite il quale si sta per procedere ad acquistare il prodotto sono utilissime.

Utilizzare, se possibile, le carte ricaricabili come metodo di pagamento

Utilizzando tale metodo di pagamento si rischia in caso di truffa di perdere unicamente il plafond disponibile sulla carta. Inoltre per effettuare una transazione online sono indispensabili pochi dati come numero di carta, data di scadenza della carta ed indirizzo per la spedizione della merce.

Occhio al "*phishing*"

Hai ricevuto una mail che richiede i tuoi dati personali o credenziali d'accesso? Non rispondere. Se ricevi mail in cui vengono richiesti dati personali, username e password del servizio di home-banking, non rispondere mai, anche se il mittente sembra essere davvero un istituto di credito: le banche non chiederanno mai via mail le tue credenziali di accesso al servizio di home-banking, gli estremi delle tue carte di credito o altre informazioni personali. In caso di dubbio, contatta direttamente il tuo istituto di credito.

Non fornire mai i propri documenti

È bene consegnare copia dei propri documenti solo se strettamente necessario ed solo se certi della affidabilità con cui vengono trattati i tuoi dati personali. Inoltre, in caso di variazione dell'indirizzo di residenza, comunica tempestivamente il tuo nuovo recapito alla tua banca e a tutti i soggetti con cui intrattieni rapporti.

Controlla spesso il tuo conto corrente

Attiva tutti gli strumenti di controllo sulle operazioni del conto, con comunicazione via messaggio delle operazioni oltre una certa soglia e, in ogni caso, abbi cura di controllare frequentemente il tuo estratto conto. Segnala subito alla tua banca eventuali transazioni che non riconosci.

Le regole sopra richiamate ridurranno notevolmente le possibilità che tu possa incorrere in una truffa, ma nel caso in cui sia stato vittima di condotte fraudolente ti consigliamo di:

- Avvisare subito il tuo Istituto di credito, bloccando eventuali carte di pagamento o disconoscendo eventuali disposizioni di bonifico non riconducibili alla vostra attività.
- Presentare immediata denuncia-querela alle autorità competenti, preferibilmente presso la Polizia Postale.
- Stampare tutti i documenti contabili che evidenziano l'operazione fraudolenta subita.

- Stampare tutte le conversazioni intercorse in caso di truffa avvenuta per mezzo di mail, sms o chat *whatsapp*.
- Rintracciare eventuali numeri di telefono da cui si sono ricevute eventuali chiamate sospette, annotando data ed ora.
- Evitare di rispondere ad ulteriori mail o telefonate sospette. Eventuali chiamate o mail da parte di soggetti che offrono aiuto per recuperare il maltolto sono anch'esse fraudolente.
- Contattate chi può fornirvi informazioni sulle frodi informatiche ed avviare le necessarie azioni tese al recupero di quanto indebitamente sottratto.

LE FRODI SUL WEB IN SARDEGNA

Il diffondersi dell'epidemia da Covid-19 ha senz'altro inciso anche sulla qualità e quantità dei fenomeni legati al *cybercrime* in Sardegna con particolare riferimento al crimine di tipo economico-finanziario.

Il *phishing* finanziario ha fatto registrare decisi incrementi anche nella nostra isola, essendo aumentata la misura delle carte di credito compromesse e dei dati finanziari commercializzati sul *web*, così come sono in aumento i casi di *vishing*, volti a carpire dati personali e codici bancari dispositivi attraverso semplici truffe telefoniche operate da numeri telefonici apparentemente riconducibili a banche ed istituti finanziari.

In via generale, vi è stato un aumento considerevole nel numero di e-mail di *phishing* in tutto il mondo con utilizzo dei temi correlati al Coronavirus per colpire persone e aziende. Di queste, un gran numero puntava su siti-clone, inducendo gli utenti di Internet a digitare le proprie password. La restante parte dei casi ha riguardato, per lo più, l'utilizzo di temi correlati al Covid-19 all'interno di messaggi email che inducevano a cliccare su allegati contenenti *malware* di varia natura.

Le nostre Sedi

ADICONSUM Sardegna

Piazza Roma pal. SOTICO piano 1° - 09170 Oristano (OR)

Tel. 078373945

Fax: 0783090224

Cell./whatsapp: 391 4950759

Email: sardegna@adiconsum.it

Pec: adiconsumsardegna@legalmail.it

Pagina Facebook: *Adiconsum Sardegna*

Cittadinanzattiva Sardegna ODV ETS

Via Ariosto, 24 - 09129 Cagliari (CA)

Tel. 070486118

Fax: 070482526

Cell./whatsapp: 370 1281722

Email: cittadinanzattiva.sardegna@gmail.com

Pec: cittadinanzattivasa1@pec.sardegnasolidale.it

Pagina Facebook*: Cittadinanzattiva Sardegna ODV ETS*

MOVIMENTO DIFESA DEL CITTADINO DI CAGLIARI

Via Pierluigi da Palestrina 30 - 09129 Cagliari (CA)

Tel./Fax 0703517990

Cell./whatsapp: 324 0976316

Email: cagliari@mdc.it

Pec: cagliari@pec.mdc.it