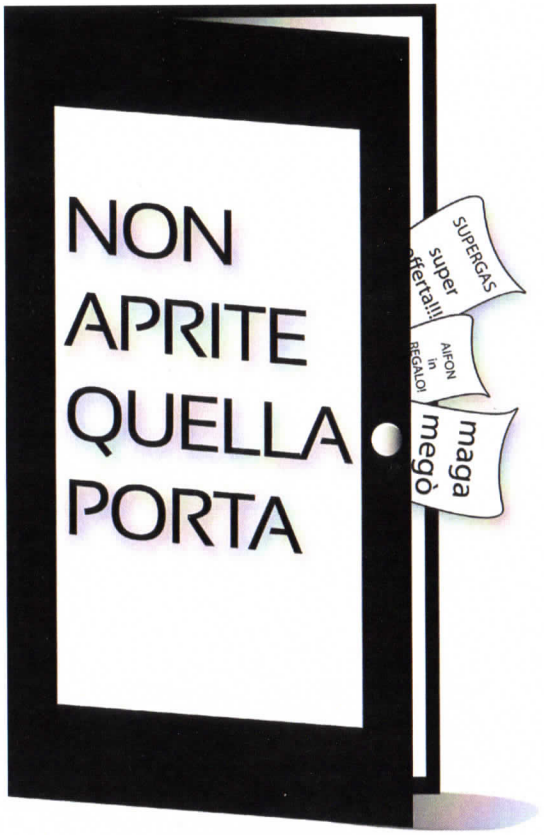
Pubblicazione a cura dell'Adoc Nazionale

Sede Nazionale: Via di Tor Fiorenza, 35 - 00199 Roma
Tel: 06/45420928 Fax: 06/86329611
Sito Web: www.adoc.org
E-mail: info@adoc.org



Suggerimenti utili per prevenire le truffe o i raggiri

NON APRITE QUELLA PORTA

Suggerimenti utili per prevenire le truffe o i raggiri

Redazione dei testi realizzata da Manuela Invidiato e Sonia Di Simine
Copertina ideata e realizzata da Flavio Mollicone
Impaginazione di Flavio Mollicone.

Pubblicazione a cura dell'Adoc Nazionale
Sede Nazionale: via di Tor Fiorenza 35 - 00191 Roma.
Tel. 06/86398975 - 06/86327211 - fax 06/86329611
Sito internet: www.adoc.org - E-mail: info@adoc.org

Progetto realizzato con il contributo del Fondo per l'Associazionismo (ex l. 383/2000) - Ministero del Lavoro e delle Politiche Sociali - Direttiva 2011

subito la banca o il gestore di carta di credito;
10. Segnalate immediatamente all'Autorità Giudiziaria o di Polizia ed alla propria Banca il ricevimento di e-mail aventi scopi o contenuti fraudolenti; è sempre consigliabile in questi casi modificare ID e password dei conti di Internet banking, preferibilmente contattando la banca. Nel caso di frode che interessi la carta di credito, fatela immediatamente bloccare dalla società emittente, chiamando l'apposito numero;

11. Diffidate in caso di improvvisi cambiamenti di modalità con la quale vi viene chiesto di inserire i vostri codici di accesso al servizio di Internet Banking, soprattutto se ciò non avviene tramite la pagina ufficiale del sito.

5. usate password diverse: non usate la stessa password per accedere a più siti e servizi sul web e non usate mai le password dei conti correnti online per l'accesso ad altri siti. Evitate, inoltre, di usare come password informazioni facilmente identificabili quali data di nascita o nome dei figli. Proteggete sempre le password e non annotatele dove potrebbero essere facilmente prelevate;

6. evitate il "salvataggio automatico" delle credenziali di autenticazione o delle password nelle memorie del personal computer utilizzato per la navigazione. È opportuno verificare che la funzione di "completamento automatico" del browser non risulti attiva;

7. adottate programmi che prevedano filtri per la posta indesiderata, in modo da filtrare e-mail inviate con scopi illeciti o pericolose;

8. utilizzate e mantenete aggiornato un idoneo Antivirus che è in grado di intercettare ed annullare eventuali programmi pericolosi; l'aggiornamento si può fare online in pochi minuti e gratuitamente cliccando sul messaggio che appare periodicamente sullo schermo all'accensione del PC;

9. controllate sempre i rendiconti: al primo segno di movimenti di denaro sospetti o pagamenti non autorizzati, anche di piccolo importo, a soggetti sconosciuti, avvisate

PREMESSA

Sempre più spesso, purtroppo, si verificano raggiri e truffe a danno di anziani, nella maggior parte dei casi con un reddito medio – basso, truffe che sono fatte approfittando dell'età, della solitudine e della debolezza delle persone.
Queste truffe possono assumere caratteristiche molto diversificate, presentarsi con modalità tradizionali o moderne, usando gli ultimi ritrovati della tecnologia informatica. Si tratta di imbrogli sofisticati messi a segno da falsi operai o dipendenti dell'Inps, finti poliziotti o medici di inesistenti organizzazioni umanitarie, che potrebbero trarre in inganno anche le persone più attente. Gli anziani, che hanno minor prontezza di riflessi e minore conoscenza di nuovi aspetti della società, vengono raggirati con maggior frequenza. Si calcola, infatti, che il 70% dei tentativi di truffe nei loro confronti, purtroppo, ha successo. È importante, quindi, saper riconoscere le situazioni più a rischio, conoscere gli elementi che possono far pensare che sia in atto un tentativo di truffa e, di conseguenza, i comportamenti da assumere.
Numerose sono le iniziative a favore delle persone anziane, specialmente per contrastare le truffe finalizzate ad estorcere loro denaro. A tale scopo vengono realizzate attività di prevenzione ad opera di Ministeri, questure, comuni e enti privati, che si impegnano per prevenire le truffe o i raggiri di cui spesso rimangono vittime e per evitare di farli sentire abbandonati. Lo scopo della guida è quello di offrire un aiuto concreto per riconoscere le situazioni rischiose che si possono incontrare nella quotidianità e, soprattutto, suggerire i comportamenti più utili per evitare spiacevoli sorprese.

INDICE

ni personali o riservate, per motivi non ben specificati (scadenza dei codici, smarrimento, problemi tecnici o di sicurezza); fanno, inoltre, spesso uso di toni "intimidatori", come minacce di sospensione del servizio in caso di mancata risposta e non riportano una data di scadenza per l'invio delle informazioni;

3. a ricevimento di messaggi e-mail, evitate di attivare i link presenti nei messaggi o di aprire file allegati alle e-mail. I link presenti nelle e-mail ricevute potrebbero condurvi ad un sito contraffatto, difficilmente distinguibile dall'originale, mentre i files potrebbero comportare rischi. In genere, basta sfiorare il link (senza mai cliccare) con il cursore del mouse per vedere visualizzato sulla barra degli indirizzi un URL decisamente sospetto, composto di una quantità di lettere e numeri che sicuramente non possono indicare un dominio web affidabile. È sempre meglio digitare l'indirizzo completo della banca nel browser. In questo modo si ha la certezza di essere sul sito ufficiale che garantisce la massima sicurezza;

4. durante la navigazione in internet evitate di fornire informazioni finanziarie o dati riservati. Prima di inserire password o numeri di carte di credito/debito in un sito web verificate che il protocollo di trasmissione sia sicuro e che il sito web risulti autentico. In questo caso è sufficiente controllare la presenza del prefisso HTTPS:// nell'indirizzo web e che sia evidenziata l'icona a forma di "lucchetto chiuso" di colore oro;

• installazione sul personal computer dell'utente di programmi in grado di produrre danni seri al terminale. Ne esistono varie tipologie, come diversi sono gli effetti dannosi che ne possono conseguire:
- alcuni di questi programmi riescono a registrare i tasti premuti dall'utente al fine di raccogliere password, numeri di carta di credito e altre informazioni personali. I più sofisticati sono in grado di monitorare anche le applicazioni usate dall'utente e i siti visitati;
- programmi maligni detti "Trojan", sono pericolosi virus che, una volta scaricati, si installano sul computer e possono creare danni notevoli. Spesso arrivano via email, chat room o download di file musicali. Alcuni Trojan usano le informazioni che trovano sul PC per reinviare copie di se stessi agli indirizzi contenuti nella rubrica email dell'utente. I più insidiosi raccolgono informazioni personali dai file che risiedono sul PC o registrano ciò che l'utente digita sulla tastiera.

Regole fondamentali per evitare le truffe sul web

1.Nessuna banca richiede codici, password o altre informazioni riservate tramite e-mail: diffidate, dunque, di e-mail, anche se ricevute da mittenti conosciuti, dove vengono richiesti dati riservati;

2.Verificate preventivamente il mittente delle e-mail: è possibile riconoscere le truffe attuate via e-mail, in quanto, generalmente, queste non sono personalizzate e contengono messaggi generici di richiesta di informazio-

1.I FALSI FUNZIONARI

È forse la più classica delle truffe. Con la scusa di un controllo dell'impianto elettrico o del gas, di una vincita improvvisa, della consegna di un pacco, o della vendita di prodotti, potrebbero cercare di introdursi in casa persone malintenzionate, a volte spacciandosi addirittura per forze dell'ordine. Prima di aprire la porta verificate l'identità della persona, controllando dallo spioncino ed utilizzando sempre la catena di sicurezza. Anche se la persona si presenta indossando una divisa, richiedete le generalità e contattate telefonicamente l'ente al quale dice di appartenere per verificarne l'attendibilità.
Le false identità assunte più frequentemente dai truffatori sono:
a) Operatore delle aziende di acqua, luce, gas, con il pretesto della lettura dei contatori o per effettuare un sopralluogo all'impianto simulando la presenza di un guasto o ancora per verificare se si effettua la raccolta differenziata. Questi truffatori spesso viaggiano con mezzi di trasporto, furgoncini o autovetture, con scritte e loghi simili agli originali che possono trarre in inganno. Una volta entrati in casa vi fanno credere con convincenti argomenti che il vostro contatore è obsoleto o ha un guasto e che, quindi, si deve procedere alla sostituzione, che ha un costo di 100 o 200 euro. Incassata la somma i sedicenti tecnici comunicano che torneranno per cambiare il contatore, lasciando nelle mani del malcapitato una falsa ricevuta

o un preventivo;
b) Funzionari INPS o Agenzia delle Entrate. Gli argomenti dei truffatori sono diversi, come la necessità di dover controllare la posizione pensionistica o contributiva, la prospettiva di un aumento di pensione, la minaccia che la pensione stessa possa essere ridotta o addirittura revocata in caso di mancato controllo, la necessità di conoscere le coordinate del conto bancario o postale per accreditare somme, e così via;
c) I finti carabinieri. Una o più persone, si qualificano come appartenenti all'Arma dei Carabinieri o alla Polizia di Stato o ancora alla Polizia Municipale, con la scusa di effettuare un controllo su delle banconote false che sono state ritirate alla banca o alla posta. Vi chiedono di poter verificare tutti i soldi che avete prelevato e poi, abilmente, li sostituiscono con banconote false o con fotocopie a colori.
Non fidatevi, nessuna banca o ufficio postale manda dei propri dipendenti o degli agenti per rilevare un errore nel conteggio del denaro che vi ha consegnato o per controllare che le banconote non siano false.
Prestate la massima attenzione anche nel caso in cui dovessero indicare con precisione la filiale della banca in cui avete il conto o in cui è stato effettuato il prelievo, questi truffatori sono abilissimi e spesso si appostano davanti alla banca, individuano la vittima e quindi successivamente sono in grado di descrivere addirittura l'impiegato.
In questi casi l'importante è essere prudenti:
• se la persona tenta di farsi ricevere in casa, non fatela

9.TRUFFE INFORMATICHE

Negli ultimi anni lo scenario delle minacce in rete è completamente cambiato. Sono aumentate notevolmente le truffe via web e sono emerse vere e proprie organizzazioni criminali dedite direttamente alle frodi online o anche alla vendita al miglior offerente di identità sottratte alle vittime.
Oggi più che mai bisogna guardarsi da forme di truffa e raggiro sempre nuove che sfruttano le "opportunità" offerte dall'innovazione tecnologica e la scarsa sicurezza della rete.
Le frodi informatiche possono essere realizzate con varie modalità:
• il phishing è una frode informatica ideata allo scopo di appropriarsi di username e password altrui al fine di effettuare operazioni bancarie. La frode è attuata dai truffatori tramite l'invio di una email ingannevole, ma all'apparenza autentica, che invita a comunicare informazioni riservate. L'email sembra provenire dalla banca o da un ufficio postale e viene utilizzato il logo, il nome e la grafica tipica della banca imitata. Queste e-mail invitano il destinatario a collegarsi, tramite l'attivazione del link contenuto nel messaggio, ad un sito Internet del tutto simile a quello della banca, dove vengono richieste le informazioni riservate. Una volta inseriti codici di accesso o numeri di carte di credito, queste informazioni sono inviate al truffatore che le può usare per svuotare conti correnti bancari o fare acquisti online;

vimenti sospetti e denunciarli alle autorità. Molte banche offrono la possibilità di monitorare l'estratto conto in tempo reale tramite internet. Inoltre, per evitare il furto e la clonazione di carta di credito e bancomat, molte banche hanno messo a disposizione dei clienti alcuni servizi come la notifica tramite Sms: a ogni utilizzo della carta di credito o del bancomat, il titolare riceve automaticamente sul proprio cellulare un messaggio di conferma e può così verificare in tempo reale i prelievi, bloccando le eventuali operazioni sospette;

6. se si subisce il furto della carta o del bancomat, bloccarli immediatamente, telefonando ai numeri predisposti dall'istituto di credito e, a seguire, fare la denuncia alle autorità (polizia, carabinieri). Una copia della denuncia dovrà poi essere inviata alla banca;

7. memorizzare il Pin e non conservarlo scritto e, comunque, mai insieme alla carta.

La clonazione della carta di credito o del Bancomat può avvenire anche utilizzando i dispositivi Pos di pagamento. Per effettuare la clonazione i dispositivi di pagamento vengono manipolati elettronicamente in modo tale da riuscire a prendere tutti i dati relativi alla carta.

Per limitare i danni della clonazione della carta di credito/bancomat si consiglia di fissare il plafond di spesa mensile al minimo indispensabile. Molte banche mettono a disposizione speciali carte di credito ricaricabili che limitano al minimo il rischio di subire danni, poiché offrono la possibilità di caricare la carta di importi molto bassi.

entrare;

- chiedete il nome della persona, la sede dell'ente a cui dichiara di appartenere ed il motivo per cui si è presentata;
- controllate telefonicamente presso l'ente dichiarato l'attendibilità di tali notizie;
- se venite contattati telefonicamente da un presunto funzionario, che vi sottopone richieste di carattere personale o patrimoniale, che possono sembrare sospette, non rilasciate alcun dato personale.

È importante sapere che non sussiste nessun obbligo di far entrare in casa operatori o funzionari di enti pubblici o privati o di associazioni, senza aver verificato prima la loro reale identità.

Il più delle volte può essere sufficiente la comunicazione, a chi vuole entrare in casa, di voler verificare la sua identità o di voler chiamare un vicino o un parente, per far allontanare queste persone, se si tratta di malintenzionati.

Ricordate che nessun ente manda personale a casa per il pagamento delle bollette o per rimborsi e, in ogni caso, prima di procedere a controlli presso le abitazioni, gli enti affiggono degli avvisi nel palazzo o contattano direttamente e in anticipo le persone per fissare un appuntamento. Anche negli ultimi casi descritti è opportuno chiedere conferma dell'attendibilità degli interventi rivolgendosi direttamente agli enti in questione.

2.VENDITORI PORTA A PORTA

Sempre più spesso capita che alla porta delle abitazioni si presenti un operatore di società di vendita di energia elettrica e metano oppure società del settore della telefonia che offrono promozioni per tagliare il costo delle bollette. Spesso, però, queste società promettono grossi risparmi al solo scopo di farsi firmare un nuovo contratto di vendita. Può capitare che si facciano consegnare una bolletta, dalla quale copiano i dati e, in alcuni casi, falsificano la firma dell'utente.
Per evitare di incappare in spiacevoli sorprese è consigliabile:

- non firmare nessun documento, né per strada né in casa, se non lo avete fatto esaminare prima dai vostri figli o da vicini di cui vi fidate;
- esigere sempre che chiunque si presenti presso la vostra abitazione si identifichi con un documento o un tesserino dell'azienda;
- non mostrare in nessun caso le bollette, perché vi sono riportati i dati dell'utente e della fornitura;
- non permettete l'accesso al contatore. Questo è consentito solo ai fini della lettura periodica dei consumi o per manutenzione (nel caso di contatore elettronico la lettura avviene a livello centrale).

In ogni caso ricordate che, come per gli acquisti a distanza (internet, telefono, televisione), è sempre possibile esercitare il diritto di recesso inviando una raccomandata

8.CLONAZIONE BANCOMAT/POSTAMAT

La clonazione della carta di credito o del bancomat/postamat è una frode molto diffusa. Le truffe si basano su sistemi sempre più sofisticati e complessi e lo scopo è quello di carpire il numero della carta ed il codice segreto. Il rischio del raggiro nel fare prelievi allo sportello bancomat è elevato. Per evitare le truffe è consigliabile:
1. non affidare il bancomat o la vostra carta di credito a nessuno;
2. non comunicare a nessuno il codice Pin del bancomat o della carta di credito e cercare di conservare il Pin separato dal bancomat o dalla carta di credito;
3. agli sportelli bancomat verificare che nelle immediate vicinanze degli sportelli non vi siano persone ferme in atteggiamento sospetto. Coprite sempre la mano quando digitate il codice;
4. prestare attenzione allo sportello, qualora presentasse anomalie, tipo rialzi della tastiera o manomissioni. Se lo sportello bancomat non restituisce la carta, chiamate subito il numero verde per bloccarla, senza allontanarsi dallo sportello stesso, mettendo in guardia altri utenti che intendessero eseguire operazioni presso lo stesso sportello, evitando inoltre che la carta stessa possa essere recuperata e successivamente clonata dai malfattori;
5. controllare l'estratto conto ogni settimana, in questo modo sarà possibile accorgersi immediatamente di mo-

7.FURTI IN AUTOMOBILE

Quando si è in automobile evitate di lasciare borse in vista o oggetti di valore, ma nascondeteli sotto il sedile o in qualsiasi luogo che possa rendere difficile il furto, inoltre, durante la sosta ad un semaforo tenete la portiera dell'auto in sicurezza ed i vetri dei finestrini alzati.
Evitare di lasciare in auto, bene in vista, monete, telefonini, occhiali e qualsiasi altro oggetto che può destare interesse.
Cercate sempre di parcheggiare in aree custodite, ben illuminate, evitando zone isolate ed utilizzate antifurti o sistemi di bloccaggio che possono rendere la vita più difficile ai ladri.
Fate, infine, attenzione ai piccoli tamponamenti: spesso sono provocati volontariamente con la scusa di far scendere il conducente, meglio se anziano, per impossessarsi del veicolo o dei beni al suo interno.

con ricevuta di ritorno entro dieci giorni lavorativi dalla firma del contratto.

➢VENDITE TELEFONICHE

In alcuni casi le società di telefonia o di energia elettrica o metano concludono contratti a distanza e, nella maggior parte dei casi, via telefono. In questi casi, la società venditrice ha l'obbligo di informarvi che si sta concludendo un contratto e che state per procedere alla registrazione in cui accettate le condizioni contrattuali. Successivamente, la società interessata deve inviare presso la vostra abitazione una copia scritta del contratto e, dal momento in cui la documentazione arriva al vostro indirizzo, decorrono dieci giorni lavorativi per esercitare il diritto di recesso.

3.FACILI GUADAGNI

Diffidate sempre da persone che propongono facili guadagni attraverso investimenti o altro. Molto spesso i truffatori si presentano con un aspetto ben curato, sono educati e gentili e dichiarano di operare per istituti bancari o per finanziarie.
Non firmate nulla prima di aver consultato il parere di amici o parenti oppure di aver sottoposto il contratto ad un avvocato di fiducia. Anche in questo caso è opportuno non fornire informazioni personali e non concedere eventuali appuntamenti a tali persone, specialmente se si è soli in casa.

nessuna ragione estraete il portafoglio.
I borseggiatori possono distrarvi in molti modi: potrebbero attorniarvi con giornali, cartoni o bambini in braccio o ancora con finti malori o finte liti. Questo è uno dei modi più facili per toccarvi ovunque e borseggiarvi abilmente. Non fatevi mai ingannare dall'aspetto distinto o dai modi gentili, qualunque richiesta potrebbe essere un pretesto per farvi tirare fuori il portafogli o per mettere in evidenza orologi o bracciali.
In caso di aggressione gridate il più possibile e cercate di ricordare dei segni di identificazione utili alla successiva cattura da parte delle forze dell'ordine (l'altezza, il viso, il tono della voce, l'inflessione dialettale, la presenza di tatuaggi, segni particolari sul corpo, l'abbigliamento e la via ed il mezzo di fuga).

interno del marciapiede e il più vicino possibile al murb si complica sicuramente il loro lavoro.
Gli scippi possono essere compiuti anche a piedi, quindi, quando sentite o notate che qualcuno compie movimenti sospetti portatevi fuori dalla sua traiettoria. Sono sempre di più i casi di scippatori che agiscono in due o più, con l'auto, affiancando le vittime prescelte e strappando loro violentemente la borsa.
Nel caso in cui siete vittime di uno scippo lasciate la presa altrimenti potreste essere trascinati e travolti.
Cercate di indossare se possibile la borsa a tracolla, con l'apertura della cerniera sul davanti e in auto posizionatela tra il sedile anteriore e quello posteriore e ricordatevi di mettere sempre la sicura alle portiere.
Diffidate, inoltre, di chi sosta in luogo isolato apparentemente senza motivo.

➢BORSEGGI
I borseggiatori sono in azione sempre più spesso e praticamente un po' ovunque, lungo le strade ma anche sui mezzi pubblici. Spesso operano in gruppo, spintonando, urtando, per poi allontanarsi rapidamente.
Soprattutto in autobus, in una fila ad uno sportello o in posti affollati state attenti alle persone che vi spingono o vi premono e cercate di non tenere il portafogli nella tasca posteriore dei pantaloni o in borse o borsellini che si aprono con facilità.
Non fermatevi in strada con sconosciuti che vi bloccano con la scusa dell'ora o del cambio di una banconota e per

4.PRELIEVO O VERSAMENTO, ALLA POSTA O IN BANCA

Quando fate operazioni di prelievo o versamento in banca o in un ufficio postale, possibilmente fatevi accompagnare, soprattutto nei giorni in cui vengono pagate le pensioni. Non fermatevi mai per strada per dare ascolto a sconosciuti che cercano di distrarvi.
Se avete il dubbio di essere osservati fermatevi all'interno di un esercizio commerciale, della banca o dell'ufficio postale, parlatene con gli impiegati o con chi effettua il servizio di vigilanza.
Durante il tragitto di andata e ritorno dalla banca non fermatevi con sconosciuti, mettete il denaro in una tasca interna dell'abito e tenete un portamonete con pochi spiccioli a portata di mano per usarlo nelle spese o eventualmente darlo in caso di rapina.
Può capitare che dopo essere usciti dalla Banca o dalla Posta o dopo avere fatto un prelievo al bancomat, si avvicini un uomo o una donna, che dice di essere un impiegato della banca o della Posta e che le banconote appena ritirate sono false. Vi chiede, quindi di controllare le banconote che poi abilmente sostituisce con banconote false o con fotocopie a colori.
Ricordatevi che nessun cassiere di banca o di ufficio postale vi insegue per strada per rilevare un errore nel conteggio del denaro che vi ha consegnato.

5.MAGHI E CHIROMANTI

L'attività di veggenti, santoni, maghi, chiromanti ed astrologi a volte può nascondere delle vere e proprie truffe. Queste persone disoneste approfittano di particolari situazioni di debolezza come difficoltà economiche o problemi sentimentali.
Per evitare inganni e furti è consigliabile:
•non dare mai i propri dati personali. Qualsiasi informazione può essere usata per minacce o ricatti;
•non incontrare mai queste persone da soli e possibilmente registrare ogni conversazione, anche telefonica;
•per eventuali pagamenti, non usare mai contanti, perché il pagamento non è dimostrabile;
•non firmare nulla;
•non aver paura di denunciarli;
•in caso di truffa o tentata truffa rivolgersi all'autorità competente.

6.SCIPPI E BORSEGGI IN STRADA

Borseggi e scippi sono tra le azioni più fastidiose e pericolose che la microcriminalità commette contro i cittadini. Ci sono, però, delle piccole tecniche che chiunque può adottare per cercare di riconoscere persone sospette oppure delle abitudini che è meglio evitare per non facilitare il lavoro di tali malfattori.
È sempre meglio evitare strade isolate e poco illuminate e di portare borse e pacchi pesanti che impediscono di muoversi con facilità. Quando si è per strada è necessario prestare attenzione alle persone che si incrociano, evitando di apparire sbadati e distratti. Se si ha l'impressione di essere seguiti è meglio entrare in un negozio o chiedere aiuto ai passanti o ad un poliziotto.
Quando si cammina sul marciapiede è preferibile andare nel senso opposto alla marcia dei veicoli, in modo da vedere chi vi viene incontro e tenersi dalla parte più vicina al muro.
In ogni caso evitare di fare sfoggio di gioielli vistosi e di portare con se molto denaro contante ma solo la somma necessaria per effettuare gli acquisti; se è inevitabile, cercare di non tenerlo tutto solo nel portafogli, ma distribuirlo tra borsa, tasche e altro.

➢SCIPPI
Gli scippatori generalmente operano in moto o motorini, quindi, per quanto abili, hanno bisogno di un minimo di spazio per agire. Camminando con le borse rivolte al lato