

Breve manuale antitruffe e consigli per la sicurezza





Numero unico a distribuzione gratuita. Realizzato da Fap Acli Firenze via Giovanni da Cascia 27 - Firenze. Stampato il 15 febbraio 2026 da Tipografia Contini - via Garibaldi - Sesto Fiorentino - Progetto grafico e impaginazione Alessandro Casini.

SOMMARIO

• Prefazione	4
• Le truffe informatiche più diffuse: i consigli della polizia postale per evitarli	6
• Truffa dello SPID	6
• Truffa delle violazioni stradali	9
• Truffa della convocazione delle Autorità	12
• Truffa dello sportello ATM	14
• Truffa del parente in difficoltà	16
• Truffa dei falsi pacchi in consegna	19
• Proposte di investimenti truffaldini: il falso trading online	21
• Truffa del curriculum	24
• Truffa del lavoro facile o dei like	25
• Quali rimedi per chi è stato truffato?	29
• La perdurante insidia delle truffe “tradizionali”	31
• Sicurezza = Qualità della Vita	37

Prefazione

Abbiamo realizzato questo piccolo manuale a diffusione gratuita e di facile consultazione con l'intervento di autorevoli esponenti delle Forze dell'Ordine che ringraziamo per averci dato i consigli utili a mettere in guardia la gente contro i tentativi di truffa, con specifico riferimento agli anziani che sono particolarmente presi di mira.

Ma, attenti ai rapporti intergenerazionali, ci siamo interessati anche dei raggiri che colpiscono soprattutto i giovani (come la truffa del curriculum) che essendo in cerca di lavoro sono più vulnerabili.

Nel frattempo, di fronte all'aumentare dei crimini informatici riteniamo che navigare online in sicurezza sia fondamentale. Quindi abbiamo dato particolare rilievo a queste situazioni perché riconoscere le minacce e adottare comportamenti adeguati è la chiave per vivere l'esperienza digitale in modo più sicuro. Ma non abbiamo dimenticato le truffe "tradizionali" che sono sempre in uso e con metodi ancor più subdoli. E abbiamo dato spazio anche alla sicurezza contro furti in casa e fuori casa che anch'essi vedono come "vittime" privilegiate gli anziani.

Inoltre, sapendo che uno dei maggiori problemi per gli anziani è quello della sicurezza in casa e fuori di casa, specialmente quando vivono da soli, abbiamo inserito una sezione dedicata specificamente ai furti e agli scippi con numerosi consigli utili per prevenirli. Nell'ambito della nostra campagna di comunicazione contro le truffe e per la sicurezza avevamo già realizzato un video che trovate nel nostro sito web <https://fapaclifirenze.it/>.

Speriamo che questo vademecum vi possa essere utile e vi invitiamo a condividerlo con i propri familiari, amici e conoscenti.



Claudio Barsacchi

Segretario provinciale
Fap Acli di Firenze

Iniziamo dalle truffe informatiche che sono quelle più “nuove” e quindi più subdole per passare poi a quelle tradizionali e a consigli su cautele da adottare contro furti in abitazioni o scippi.

Le truffe informatiche più diffuse: i consigli della Polizia Postale per evitarle

Intervista e consigli della **Dott.ssa Eva Claudia Cosentino** Primo Dirigente della Polizia di Stato, dirigente del Centro Operativo per la Sicurezza Cibernetica (COSC) Toscana.

Truffa dello SPID

Domanda: Si registra un aumento delle truffe che utilizzano il nome dell'Istituto Nazionale della Previdenza Sociale. Come avviene il raggiro?



Risposta: In genere si cerca di carpire dati personali ai destinatari di SMS o e-mail ingannevoli, apparentemente provenienti dall'INPS.

Le false comunicazioni invitano a cliccare su un link per aggiornare i propri dati: il sito su cui si viene reindirizzati è una copia di quello ufficiale dell'Istituto, ma non è autentico. A questo punto viene chiesto di inserire informazioni personali sensibili come dati anagrafici, codice fiscale, Iban, copia di documenti, un selfie o un video. Con il materiale raccolto viene creato un falso Spid, poi usato per compiere attività illecite. Si tratta di un vero e proprio furto di identità, che ha conseguenze disastrose per la vittima. Infatti, se vengono utilizzati *Identity Provider* differenti, il Sistema SPID autorizza la coesistenza di più identità valide per lo stesso codice fiscale.

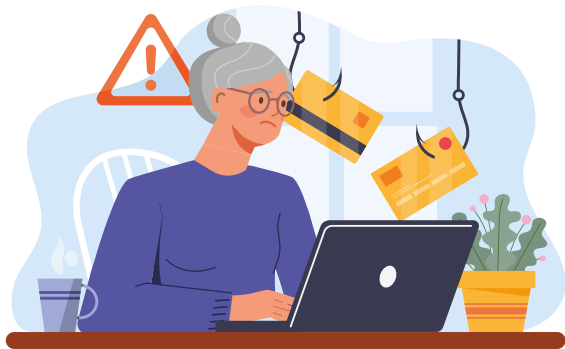
È bene sapere che le notifiche ufficiali dell'Istituto inviate tramite SMS, relative agli esiti di lavorazione delle pratiche o ai pagamenti, non contengono mai link cliccabili.

Gli SMS inviati hanno esclusivamente una funzione informativa, per segnalare la presenza di nuove comunicazioni disponibili per la consultazione. Questi messaggi non contengono mai alcun collegamento ipertestuale attivo. Per accedere alle informazioni dettagliate riguardanti le proprie pratiche e i pagamenti, gli utenti possono utilizzare l'area riservata MyINPS.

Come difendersi:

- ◇ Non cliccare MAI su link contenuti in messaggi di testo o di posta elettronica: si tratta di tentativi di *phishing* o *smishing*, volti a carpire alle vittime dati e informazioni riservati.
- ◇ Non rispondere ai messaggi che richiedono informazioni personali o finanziarie.
- ◇ Se ricevete un SMS sospetto, segnalatelo immediatamente al vostro provider di telefonia mobile.
- ◇ Bloccare il mittente dei messaggi sospetti, prevenendo ulteriori contatti.
- ◇ Assicuratevi che il software del telefono sia sempre aggiornato all'ultima versione per proteggervi da nuove minacce.
- ◇ Non fornire copia dei propri documenti d'identità.

Truffa delle violazioni stradali



Domanda: Un raggiro assai diffuso è la presunta violazione del codice della strada, ma come viene attuato?

Risposta: Si tratta di attacchi informatici mirati: e-mail e SMS apparentemente istituzionali che simulano la comunicazione di una sanzione, in genere una presunta infrazione del codice stradale. Il messaggio invita a pagare tramite un portale fittizio che imita in modo estremamente credibile l'interfaccia di pago-PA. Il sito fraudolento, raggiungibile da un link incluso nel messaggio, riproduce fedelmente grafiche, colori e font del portale ufficiale, ma è ospitato su domini creati ad hoc con l'obiettivo di sottrarre informazioni personali e bancarie.

Una delle caratteristiche che rende questo attacco particolarmente insidioso è il tono della comunicazione: la grammatica è curata, il linguaggio è formale, e l'e-mail include riferimenti numerici molto simili ai reali codici di violazione (es. #R7230033407). Inoltre, viene indicato un importo e paventata un'eventuale maggiorazione se il pagamento non venga effettuato in tempi rapidi. Invita a cliccare su un link per accedere al portale del pagamento con cui regolarizzare la propria posizione il prima possibile. Si sfrutta l'urgenza per indurre le potenziali vittime a compiere azioni senza riflettere.

Come difendersi:

- ◇ Quando viene intimato un pagamento, accertarsi che sia legittimo contattando l'ente da cui sembra provenire il messaggio.
- ◇ Anche se l'e-mail sembra provenire dalla piattaforma pagoPa: verificare che il pagamento sia dovuto, accedendo direttamente al sito ufficiale e controllare la URL del sito.
- ◇ Diffidare di comunicazioni che chiedono pagamenti urgenti e informazioni personali.
- ◇ Le truffe online fanno leva sull'urgenza per portarvi a compiere azioni impulsive. La prima regola è quindi quella di non lasciarsi prendere dal panico.
- ◇ Non aprire link sospetti e non inserire mai dati

personali e/o sensibili – come numeri di carta o credenziali bancarie: pagoPA non richiede mai tali informazioni tramite messaggi recapitati via e-mail o SMS. Il dominio ufficiale di pagoPA è *checkout.pagopa.it*.

- ◇ Anche l'analisi del testo può offrire indizi: toni troppo allarmistici, mancanza del certificato di sicurezza *https*, caratterizzato dalla presenza del lucchetto nella barra degli indirizzi del *browser*, che permette di distinguere un sito sicuro da uno pericoloso.
- ◇ Controllare il mittente dell'e-mail: gli indirizzi autentici di pagoPA sono riconoscibili, ad esempio *noreply-checkout@ricevute.pagopa.it*. Fare attenzione anche a eventuali piccole variazioni, errori ortografici o inconsistenze palesi (ad esempio provengono da un mittente che ha un nome e un cognome creato ad hoc).
- ◇ Se nonostante queste accortezze non si riesce ancora a capire se il messaggio di posta elettronica ricevuto sia genuino, può essere inoltrato al CERT-AgID, all'indirizzo:
malware@cert-agid.gov.it oppure
malware@cert-agid.gov.it così da ricevere assistenza.

Truffa della convocazione delle Autorità



Domanda: Come avviene?

Risposta: Ci si vede notificare un avviso di un'inchiesta per un presunto “utilizzo improprio della rete” vengono avanzate accuse gravi, come il coinvolgimento in reati di pedopornografia. A volte viene paventata l'iscrizione in registri inesistenti, come il “Registro dei delinquenti sessuali”. Tutto questo mira a generare panico e a ottenere una risposta impulsiva. A volte, la minaccia è amplificata prospettando conseguenze gravi, come l'arresto. In alcuni casi, i truffatori allegano documenti falsi, come presunti mandati

di arresto o rapporti d'indagine, per far crescere ulteriormente la pressione psicologica e spingere l'utente a mettersi in contatto con il truffatore. È qui che scatta la seconda fase della truffa: la richiesta di pagamento di una somma di denaro per "risolvere" la situazione. Si sfruttano il nome delle Autorità, come il Capo della Polizia, la Polizia Postale, i Carabinieri, etc. e i loghi ufficiali, apparentemente autentici, per intimorire le vittime. Ma nessuna Forza di Polizia contatta direttamente i cittadini, attraverso e-mail o sms, per chiedere dati personali o pagamenti in denaro, con la minaccia di procedimenti penali a loro carico.

Come difendersi:

- ◇ Mantenere la calma e analizzare il messaggio ricevuto: solitamente, la denominazione della presunta Autorità è simile, ma non conforme a quella autentica.
- ◇ Diffidare delle richieste urgenti di pagamento e del linguaggio intimidatorio.
- ◇ Non rispondere al messaggio e non seguire le istruzioni che contiene, ovvero non cliccare su eventuali link, non fornire dati personali, non scaricare eventuali allegati e, naturalmente, non pagare le cifre richieste.
- ◇ Denunciare l'accaduto alla Polizia Postale o a qualsiasi forza di Polizia.

Truffa dello sportello ATM

Esiste da tempo ma è sempre insidiosa.



Domanda: Quali cautele da adottare?

Risposta: Il meccanismo segue uno schema preciso: il truffatore, fingendosi interessato ad acquistare un bene messo in commercio online, chiede al venditore di poter pagare su conto corrente o su una carta ricaricabile e, una volta ricevuto l'assenso, inviterà la vittima a recarsi allo sportello ATM “per controllare o confermare l'accredito”.

D: Questa richiesta dovrebbe già insospettire?

R: Infatti, per effettuare un bonifico o una ricarica, bastano nome, cognome e l'IBAN del conto o il numero della ricaricabile, senza necessità di recarsi fisicamente presso uno sportello ATM. A questo punto, il truffatore chiede di accedere al conto del venditore dall'ATM e di selezionare la voce "effettua ricarica". Indica poi un codice alfanumerico, che spacerà per il numero dell'ordine da verificare (in realtà, sta comunicando il suo IBAN o il numero della sua carta).

Come difendersi:

- ◇ Tenere sempre a mente che non esiste alcun servizio Bancomat, né di Poste Italiane, né di altri istituti di credito, che permette di controllare lo stato degli ordini online da un distributore automatico.
- ◇ Ricordare che nessun pagamento online richiede al beneficiario di recarsi personalmente al Bancomat per concludere l'operazione. In caso di simili richieste, si tratta di un tentativo di truffa: la somma che l'interlocutore chiede di inserire corrisponde al prezzo pattuito per la vendita online, ma, di fatto, sta chiedendo di trasferirgli quella cifra sul suo conto.

Truffa del parente in difficoltà



Un tentativo di raggiro particolarmente odioso perché fa leva su uno stato d'animo di ansia e di apprensione. L'inganno inizia con l'invio alla vittima di un SMS o messaggio WhatsApp, con cui, quello che si presenta come un parente prossimo, di solito un nipote o un figlio, asserisce di aver subito il furto (o di aver smarrito) il cellulare, indica il nuovo numero e chiede soldi, adducendo le ragioni più disparate: non riesce ad accedere al conto corrente e ha urgente bisogno di effettuare pagamenti, è rimasto in panne con l'auto e necessita di denaro per pagare subito il soccorso stradale, è stato fermato dalla polizia per una rissa e servono soldi per l'avvocato, etc.

Una volta innescata l'emergenza emotiva nella vittima, convincendola che il suo aiuto è essenziale, i

truffatori la inducono a effettuare versamenti di denaro attraverso bonifici istantanei, ricariche su carte prepagate o pagamenti immediati attraverso servizi di Money Transfer (Mooney, Sisal Pay, etc.).

Se la vittima sostiene di non avere disponibilità immediata di contanti, il truffatore replica che si accontenta anche di oggetti preziosi di pari valore. Talvolta si dice che bisogna versare una cauzione per evitare l'arresto, da consegnare in contanti a un finto poliziotto o carabiniere. Attenzione: A volte i truffatori si assicurano che la vittima non comunichi verso l'esterno tenendo occupata sia la linea fissa, sia il cellulare.

Come difendersi:

- ◇ Tenere a mente che la normativa italiana non prevede alcuna cauzione in caso di arresto.
- ◇ Non far entrare nessuno in casa: i truffatori potrebbero reagire in maniera violenta al rifiuto di consegnargli il denaro o i gioielli.
- ◇ Ricordarsi che le Forze dell'Ordine non chiedono denaro per assistere i cittadini
- ◇ Mantenere la calma e la lucidità: bisogna ragionare a mente fredda, senza farsi prendere alla sprovvista e senza avere fretta.
- ◇ Prendere tempo con il truffatore, adducendo scuse per non aderire alla sua richiesta.
- ◇ Contattare il congiunto che si crede essere in difficoltà: basta una telefonata o un messaggio

su WhatsApp, sul “vecchio” numero che già si conosce, per assicurarsi delle sue condizioni e che non ha subito alcun furto, incidente o arresto. Appena chiusa la telefonata, chiamare il numero di emergenza unico 112 per segnalare l'accaduto. Attenzione: si è ricevuta la chiamata truffaldina sul numero di telefono fisso, la chiamata al 112 va fatta dal cellulare, poiché di solito il malfattore non chiude il collegamento, proprio per impedire alla vittima di contattare l'esterno, quindi la vittima che compone il 112 o il numero del parente continuerebbe a parlare con il truffatore.

- ◇ Diffidare di chi chiede soldi con urgenza.
- ◇ Non fornire mai informazioni personali a sconosciuti.
- ◇ Segnalare il numero alla polizia e bloccare il contatto sospetto.

La truffa dei falsi pacchi in consegna

Per questa truffa, l'utente viene invitato a cedere le sue informazioni personali e bancarie cliccando sul link proposto all'interno di un SMS che apparentemente proviene da noti corrieri (Es.: Bartolini, Amazon, etc.):



“Ciao Maria, il tuo pacco è stato consegnato al punto di consegna. Vedi dove puoi ritirare il tuo pacco...”

Questo il testo che viene recapitato agli utenti presi

di mira dall'ultimo aggiornamento di questa campagna malevola.

Il messaggio viene poi completato con un link fraudolento che rinvia a un sito clone in cui, per accedere, viene richiesto di inserire i propri dati personali e bancari, ma lo scopo dei truffatori è di impossessarsene. In alcuni casi, l'SMS informa che un pacco è bloccato e si può sbloccarlo pagando una piccola somma (di solito 2 €).

Come difendersi:

- ◇ In caso di ricezione di comunicazioni inattese, perché magari non è stato effettuato alcun ordine, non dare seguito a messaggi come questo. Nel caso, invece, di attesa di reale pacco in consegna, effettuare i controlli mediante il servizio utilizzato per completare l'ordine. All'interno di un'area riservata, infatti, è sempre contenuto un link di tracciabilità del pacco. Così si è sicuri di venire indirizzati al reale sito del corriere e non verso una piattaforma fraudolenta.
- ◇ Tenere a mente che nessun corriere chiede soldi tramite messaggio per consegnare un pacco.

Proposte di investimenti truffaldini: il falso trading online



L'utente si imbatte, sui social network, in un annuncio che pubblicizza investimenti ad alto profitto, a volte la proposta di investimento arriva alla vittima direttamente tramite una telefonata, da parte di un sedicente broker che promuove il tipo di investimento, nonché le modalità di esecuzione, che prevedono un'assistenza completa per le procedure di versamento e di registrazione sulle relative piattaforme. Tali informazioni hanno la finalità di tranquillizzare il "cliente". La vittima viene quindi convinta a effettuare un minimo versamento, solitamente di € 250,00, per partecipare

e gli viene creato un account su una piattaforma di trading online. L'obiettivo è far eseguire direttamente alle vittime dei bonifici verso conti correnti che, secondo il sedicente broker, servirebbero a effettuare l'investimento. Spesso, il truffatore chiede alla vittima di installare sul proprio dispositivo un'applicazione dedicata, che servirà a consentire il controllo da remoto, delle operazioni volte al finto investimento. La piattaforma *fake* (fasulla) riporta anche l'andamento fittizio del presunto investimento effettuato dalla vittima, facendo sembrare che stia effettivamente fruttando. Ciò in quanto l'account fornito alla vittima per seguire gli investimenti è, in realtà, un profilo "DEMO" della piattaforma creata ad hoc dai truffatori, in cui verranno visualizzate informazioni FALSE, tra cui i profitti che risulteranno sempre più favorevoli, invogliando l'ignaro investitore ad aumentare i versamenti, che vengono effettuati mediante bonifici verso conti esteri o su portafogli di cripto valuta, gestiti direttamente dal falso *broker*. Quando poi si vuole realizzare il guadagno e si chiede di disinvestire, allora il sedicente broker fa presente che occorre un pagamento ulteriore, con il pretesto di sbloccare il capitale investito.

Come difendersi:

- ◇ Non fidarsi di telefonate o messaggi provenienti da numeri sconosciuti, soprattutto se esteri e non cliccare su link sospetti.
- ◇ Verificare l'attendibilità di chi propone l'investimento, visitando i siti della Consob e della Banca d'Italia.
- ◇ Diffidare di proposte apparentemente molto vantaggiose o di un lavoro dal facile guadagno: quando un'offerta è troppo bella per essere vera, quasi certamente, infatti, non lo è!
- ◇ Porre particolare attenzione alle offerte di lavoro per le quali non si è fatta specifica richiesta o che vengono diffuse sui social network.
- ◇ Non rispondere, bloccare i messaggi ricevuti da mittenti sconosciuti e non aprire link che potrebbero compromettere il dispositivo.
- ◇ Non condividere dati personali, bancari, credenziali di accesso, documenti d'identità con presunti agenti finanziari, banche, etc.
- ◇ Fare subito denuncia: la tempestività è fondamentale per recuperare le somme investite e tentare di identificare gli autori.

Truffa del curriculum

Questa truffa prende di mira particolarmente i giovani. Una telefonata che sembra una delle tante proposte commerciali. Invece...



È la nuova frontiera del *phishing*. Nella maggior parte dei casi, la vittima riceve una chiamata proveniente da un numero telefonico con prefisso italiano, ma possono anche arrivare e-mail o un sms, con cui viene informato che il suo curriculum è stato selezionato per un'opportunità di lavoro, invitando a proseguire la conversazione su WhatsApp.

Il falso operatore invia quindi un link, che rimanda su

una piattaforma, dove viene chiesto di inserire i propri dati personali e bancari o copia di documenti. La piattaforma è del tutto simile a quelle utilizzate per ricerche e offerte di lavoro.

Cliccando sulla piattaforma, si riceve un virus che entra in possesso del dispositivo, telefono o computer e carpisce dati personali e password, che poi consentono di effettuare operazioni finanziarie sottraendo così denaro alla vittima, oppure di accedere ai contatti presenti in rubrica.

Truffa del lavoro facile o dei like

Ci si approfitta anche del desiderio dei giovani di trovare un lavoro e di molti che vorrebbero avere entrate supplementari per arrotondare stipendio o pensione.



“Salve, posso parlarle un attimo?”, *“Ciao! Mi dispiace disturbarli! Posso avere un po’ del tuo tempo?”*

Con frasi simili le vittime vengono contattate tramite messaggi sui social oppure tramite messaggi WhatsApp da interlocutori che, utilizzando numeri esteri, proponendo offerte di lavoro che sembrano allettanti, consistenti nel guardare filmati su piattaforme social o su portali creati ad hoc dai truffatori, apporre like su foto e video segnalati, seguire profili social, scrivere recensioni, etc. Ogni like è retribuito con una piccola somma di denaro, a fronte dell’invio al “reclutatore”, come prova, degli *screenshot* dell’attività svolta. Sono questi guadagni iniziali che illudono le vittime di aver fatto un affare e che servono ai malviventi ad assicurarsi la loro fiducia. Accettata l’offerta, gli utenti vengono dapprima inseriti in gruppi social o di messaggistica istantanea e poi invitati a registrarsi su un portale, creato dai truffatori, e a inserire i propri dati personali.

A quel punto, viene prospettato che, per aumentare i guadagni, possono essere acquistati dei “crediti” che hanno valore economico e che saranno rimborsati dopo le recensioni stesse. Alla vittima il sistema sembra funzionare, perché, dopo avere acquistato falsi crediti e avere messo i like richiesti, si vedono accreditare sul loro falso account aperto dai truffatori quanto pattuito. Il problema nasce nel momento in cui chiedono di ritirare il denaro, perché a quel punto vengono richiesti altri soldi per svincolare il guadagno.

Oppure, alle vittime viene suggerito di scaricare applicazioni di messaggistica e di iscriversi a determinati canali, con la promessa di guadagni ancora più elevati, a fronte di un piccolo investimento.

Inizialmente i truffatori chiedono bonifici di poche decine di euro, che vengono rimborsati con una piccola maggiorazione. Dopo i primi bonifici chiedono d'investire somme sempre più alte con la promessa di un guadagno ancora più sostanzioso. All'invio di un bonifico con un'ingente somma da parte della vittima, il malfattore sparisce e diventa irreperibile.

Oltre al chiaro obiettivo di estorcere denaro questo genere di truffe ha anche lo scopo di rubare dati sensibili, codici bancari e password.

Come difendersi:

- ◇ Porre particolare attenzione alle offerte di lavoro per le quali non si è fatta specifica richiesta o che vengono diffuse sui social network.
- ◇ Non rispondere, bloccare i messaggi ricevuti da mittenti sconosciuti e non aprire link che potrebbero compromettere il dispositivo.
- ◇ Non fidarsi di chiamate/messaggi provenienti da numerazioni con prefisso estero.
- ◇ Verificare sempre l'azienda facendo una ricerca approfondita sulla società che offre il lavoro controllando recensioni e feedback degli utenti della rete.

- ◇ Diffidare di chi promette facili guadagni: se un'offerta è *“troppo bella per essere vera”*, quasi certamente, infatti, non lo è!
- ◇ Non inviare mai denaro: nessuna azienda seria richiederà l'invio di denaro per svolgere lavori online.
- ◇ Proteggere i propri dati personali e non condividere informazioni sensibili come numeri di conto bancario, credenziali di accesso, documenti d'identità con sconosciuti.
- ◇ Nelle impostazioni di privacy delle App di messaggistica istantanea, è bene selezionare l'opzione *“consenti solo ai miei contatti di aggiungermi sui gruppi”*, per non ritrovarsi inseriti in chat indesiderate da sconosciuti.
- ◇ Se si sospetta di essere vittima di una truffa, denunciare subito l'accaduto alla Polizia Postale o a qualsiasi altro Ufficio di Polizia.

Quali rimedi per chi è stato truffato?

Ne parliamo con l'**Avv. Francesco Parenti**, Patrocinante in Cassazione.

Il reato di truffa è previsto dall'art. 640 del Codice Penale e punisce una falsa rappresentazione della realtà per portare la vittima a fare una certa cosa oppure a non fare una determinata cosa. È uno dei reati più odiosi perché fa parte dell'ambito dei reati che richiedono necessariamente la "cooperazione" della vittima, e quindi le caratteristiche della vittima hanno un ruolo fondamentale.

Pertanto, più un soggetto è debole e fragile e più è facile ingannarlo. Sono moltissime le tipologie che possono verificarsi. Così come dopo il covid 19 si è sviluppato lo smart working, anche le truffe online hanno oramai preso il sopravvento. Quindi sono essenziali le accortezze per sventarle.

Domanda: Come possiamo comportarci quando invece il reato è stato già consumato?

Risposta: Per prima cosa occorre recarsi subito dalle Forze dell'ordine e sporgere una denuncia. Si può farlo da soli o chiedere l'aiuto di un legale specie quando la truffa si è verificata in modo complesso e

articolato: ad esempio in più giorni o in più fasi. Inoltre si consiglia, in caso di truffa informatica, di salvare tutti i file che potrebbero avere interesse ai fini della denuncia e anche portare direttamente il dispositivo informatico alle Forze dell'ordine.

La denuncia fornisce una tutela in ambito penale, e il consiglio è di farla nel più breve tempo possibile. È vero che ci sono tre mesi di tempo ma è meglio che sia tempestiva per consentire alle Forze dell'ordine e all'Autorità giudiziaria di individuare i responsabili e perseguirli penalmente.

C'è poi l'altro lato della medaglia che è l'azione per la responsabilità civile. Infatti l'anziano truffato ha ovviamente un interesse a recuperare il maltolto, il denaro o gli oggetti che ha perso e ottenere il risarcimento del danno.. Qui si aprono diverse strade, diverse strategie professionali e quindi è utile rivolgersi a un avvocato.

(conversazione tratta da intervista video)

La perdurante insidia delle truffe “tradizionali”

Ne parliamo con il Capitano dei Carabinieri **Cap. Alessandra Giardino** Comandante della Compagnia di Pontassieve (Fi).

Si tratta di truffe che sono sempre insidiose e continuano a mietere vittime e parliamo anche del tema sicurezza che è sempre più di attualità.

Riportiamo qui l'intervista effettuata in un nostro video che mette in guardia gli anziani contro i tentativi di truffa.

Domanda: A seguito delle campagne di comunicazione c'è maggiore consapevolezza e quindi più accortezza da parte della gente circa le tipologie di truffe più diffuse?

Risposta: Il fenomeno delle truffe, che colpisce in specie gli anziani, crea sempre allarme sociale perché va a intaccare le fasce più deboli. La vittima si trova di fronte a una richiesta di denaro. Essendo imprevista e urgente, tale richiesta ha l'effetto di provocare turbamento e di far diminuire la lucidità.

D: Un vantaggio per il truffatore...

R: Infatti. Le vittime, fra timore e fretta devono cercare di dare una risposta mentre il truffatore ha preparato il raggio studiando anche alcuni dettagli della vita della persona che viene presa di mira.

D: Quali le più frequenti tipologie di truffa?

R: Le truffe in generale sono un fenomeno sempre presente. Negli ultimi anni si è maggiormente sviluppato online ed è particolarmente insidioso perché non c'è un rapporto diretto fra le persone. Quindi è più difficile andare a identificare gli autori persona del raggio.

Il classico esempio di truffa online è l'acquisto di un oggetto su qualche sito che chiede un pagamento preventivo e che poi non invia l'oggetto che si è acquistato. Questo un fenomeno abbastanza diffuso anche se le persone sono sempre più attente quando fanno gli acquisti.

D: E per quanto riguarda specificamente gli anziani?

R: Il discorso sulle truffe agli anziani è uno dei più delicati. C'è un grande impegno da parte delle forze dell'ordine, per cercare di far capire a tutta la popolazione ma in particolar modo agli anziani i rischi che ci possono essere dietro queste richieste fatte da sedicenti avvocati, carabinieri, forze dell'ordine o anche impiegati di aziende di distribuzione di elettricità

o del gas.

D: Anche gli anziani, quindi, mostrano maggiore accortezza?

R: Facendo un'intensa opera di sensibilizzazione sul territorio, negli ultimi anni ho notato un notevole miglioramento nel senso che la divulgazione e l'informazione su questi temi ci ha consentito di sventare numerose truffe anche nei confronti di anziani. Quindi, un miglioramento. Ma il rovescio della medaglia è che gli autori dei raggiri si aggiornano: nel momento in cui un tipo di truffa diviene "famoso", loro cambiano i metodi. Quindi, non è sempre semplice andare a contrastare il fenomeno. Però, sicuramente, l'attività di prevenzione sta dando risultati.

D: Come accorgersi che si sta per essere vittima di una truffa? Come avviene il tentativo di raggio?

R: In genere, nella fase iniziale c'è una telefonata da parte di una persona che finge di essere un avvocato o un appartenente alle forze dell'ordine. Questi fa una richiesta di denaro affermando che c'è un parente stretto, un figlio o un nipote che ha fatto un incidente stradale o che è stato arrestato per una qualsivoglia ragione e che per essere liberato o scagionato ha urgente necessità di soldi.

D: Come evitare di cadere in una trappola così subdola?

R: In questi casi bisogna partire da un presupposto: le forze dell'ordine e comunque chi lavora nell'ambito della giustizia non fanno mai richieste di denaro. Questo è il primo elemento che deve arrecare sospetto a chi riceve queste telefonate.

Inoltre, non è possibile che dietro un pagamento di denaro una persona venga liberata. Quindi le richieste di denaro o addirittura di monili in oro in sostituzione di denaro contante fanno capire che si è di fronte a un tentativo di raggio.

Il secondo campanello d'allarme è che i truffatori cercano di trattenere il maggior tempo possibile al telefono la potenziale vittima per accrescere la condizione di pathos, di preoccupazione. Il soggetto preso di mira perde un po' di lucidità e cerca in maniera spasmodica quello che può dare. Poi, poco tempo, dopo arriverà un complice che prenderà il denaro o monili d'oro.

D: Cosa si deve fare in questi casi?

R: La prima cosa è interrompere il colloquio telefonico e chiamare il 112 o il numero della Caserma di riferimento sul territorio. In tal modo, parlando con un vero operatore delle forze dell'ordine questi facilmente fa comprendere che non può essere una

richiesta lecita quella che è stata effettuata.

Nel caso in cui questo non si riesca a fare e si cada nel tranello la cosa essenziale da fare in un secondo momento appena ci si rende conto di essere vittime di truffe è denunciare.

La denuncia è un fattore molto importante perché, intanto, per noi è il modo di iniziare l'attività investigativa e fornisce strumenti per recuperare quanto perso dalla vittima.

Si comprende che dietro al fenomeno delle truffe ci sia anche la riluttanza a denunciare perché la vittima si sente in colpa per essere caduta nel tranello. Quindi ha un po' di timore e vergogna di far sapere cosa è successo. Però per noi è importante ai fini investigativi acquisire le informazioni utili.

D: Oltre alla truffe c'è anche il problema della sicurezza. Lei ha una particolare cura per la prevenzione, oltre che per la repressione del reato, ovviamente?

R: Nel nostro territorio c'è un forte impegno da parte dell'Arma dei Carabinieri per fornire, mediante pattuglie, una protezione più ampia possibile sul territorio. E constatiamo che, con un lavoro di prevenzione, è possibile ridurre fenomeni criminosi.

I furti nelle abitazioni, per esempio: la presenza di pattuglie disincentiva a compiere questa tipologia di reati. E un altro fenomeno che viene contrastato con una rilevante presenza sul territorio è quello di furti

sulle persone, come gli scippi in strada o nei negozi. Il nostro impegno per diffondere sicurezza comprende anche l'attività per identificare gli orari e i luoghi che hanno necessità di maggiore controllo. Così, negli ultimi anni, stiamo avendo risultati positivi si è creata nel cittadino la percezione di una maggiore sicurezza. Inoltre, la prevenzione è importante anche nella sicurezza stradale perché un controllo su persone che siano nell'impossibilità di guidare per abuso di alcol o di sostanze stupefacenti impedisce che possano arrecare un danno ed evita un possibile incidente stradale.

Sicurezza = Qualità della Vita

Il **Comune di Pontassieve** ha pubblicato il Vademecum **#sicuramente** ricco di consigli per utilizzare accortezze che accrescano la sicurezza contro furti e scippi. In collaborazione con Carabinieri e Polizia Locale. Ne riportiamo sinteticamente alcune parti in questa conversazione con il **Dott. Marco Stagi** Comandante della Polizia Locale.

Domanda: Come prevenire le più frequenti situazioni di pericolo. Ad esempio i furti nelle abitazioni?

Risposta: Prima di uscire chiudere bene porte e finestre dell'abitazione, il portone d'ingresso del palazzo e/o il cancello e non informare conoscenti, né tantomeno estranei, sul tipo di dispositivo di sicurezza di cui è dotata l'abitazione. È sempre meglio attivare l'impianto di allarme e/o le videocamere sia quando esci di casa, anche se solo per breve tempo, sia la notte quando sei in casa.

All'imbrunire accendi, dove possibile, le luci esterne o utilizza sistemi luminosi alternativi di basso consumo. Tra le prime cautele quelle che riguardano le porte e le finestre... L'ingresso è importante: scegli con cura l'infilzo dell'uscio di casa e, se puoi, installa una porta blindata munita di fermaporta e spioncino, un videocitofono e un sistema di allarme e/o di videocamere; adotta idonei accorgimenti anche per le porte laterali

e quelle del garage.

Controlla sempre prima di aprire portoni e/o cancelli: diffida degli sconosciuti anche se indossano una qualche uniforme o dichiarano di essere dipendenti di aziende pubbliche; non mandare i bambini a rispondere al citofono o alla porta e non fare entrare estranei che si presentano come amici dei tuoi figli o parenti.

D: E per quanto riguarda chiavi e serrature?

R: Mai lasciare le chiavi di casa sotto lo zerbino o in luoghi esterni all'abitazione facilmente intuibili per i malintenzionati.

- Rivolgersi solo ad un ferramenta di fiducia per duplicare le tue chiavi di casa e non scrivere nome e indirizzo sul portachiavi.
- In caso di necessità non consegnare le tue chiavi se non a persone di fiducia, per evitare che qualche malintenzionato possa farne un calco.
- In caso di smarrimento delle chiavi di casa, cambiare tutte le relative serrature e gestisci il fatto con riservatezza, evitando di informare troppe persone.

In caso di trasferimento in una casa già prima abitata cambiare le serrature. Se la casa è nuova, verificare che le serrature non siano le stesse usate durante

i cantieri (le nuove chiavi dovrebbero essere consegnate in una busta sigillata).

D: Per le finestre?

R: Prediligere gli infissi esterni dotati di maniglie con serratura, meglio se collegati all'antifurto o provvisti di vetri antisfondamento. Se decidi di far installare grate fisse o scorrevoli chiedi al fabbro di non lasciare più di 12 cm tra una sbarra e l'altra. Inoltre, anche se abiti ai piani rialzati non lasciare le finestre aperte quando non sei in casa o di notte perché i ladri si calano dai tetti o si arrampicano sulle grondaie.

D: Come conservare documenti e oggetti preziosi?

R: Conservare i documenti personali (libretto degli assegni, carte di credito, bancomat, passaporto, etc) nella cassaforte o in un altro luogo sicuro e non nei classici posti.

- Differenzia i posti dove conservi gli oggetti di valore.
- Fai un accurato inventario degli oggetti di valore corredandolo di schede descrittive e fotografie e conservalo in un'abitazione di fiducia.
- Riponi con attenzione le copie dei documenti di identità e gli originali degli atti importanti.
- Non lasciare oggetti preziosi, portafogli, chiavi di casa, del garage o dell'auto in mostra in mensole e mobiletti all'ingresso dell'abitazione.

D: Accortezze da usare, all'esterno dell'abitazione?

R:

- Fare in modo che ogni giorno la cassetta della posta venga svuotata da una persona di fiducia durante i tuoi periodi d'assenza (una cassetta stracolma indica che manchi da tempo).
- Non esitare a chiamare i numeri utili delle forze dell'ordine in caso di rumori, presenze, movimenti o passaggi sospetti di autovetture segnandone, in questo caso, targa, modello e colore.
- Non lasciare scale o cavalletti a portata di mano per impedire ai ladri di usufruirne per arrampicarsi sulle condutture del gas, sulle impalcature o sulle grondaie.
- Abbi cura di mantenere buoni rapporti con i condomini o, in caso di abitazione singola, con i dirimpettai; è fondamentale la collaborazione per la sorveglianza reciproca delle proprietà, per il controllo dell'effettiva chiusura di cancelli, per lo scambio d'informazioni su eventuali ditte incaricate di eseguire lavori in tua assenza.

D: Cosa fare se si è subito un furto?

R: Se al rientro a casa scopri che c'è stato un tentativo di effrazione o un furto e ti accorgi che la serratura è stata manomessa o che la porta è socchiusa, non entrare subito per vedere “cosa hanno fatto”, poiché

all'interno dell'abitazione potrebbe esserci ancora qualcuno e potresti non essere in grado di affrontarlo in modo adeguato; meglio evitare che un "semplice" furto si trasformi in un fatto ben più grave, perciò chiama subito le Forze dell'Ordine ed evita di toccare in giro per non inquinare le prove.

D: Bisogna anche fare attenzione ai segni tracciati all'esterno?

R: Nel caso in cui rinviene segni strani sui muri o sui citofoni di casa, del palazzo o dell'azienda, chiama immediatamente le Forze dell'Ordine e in seguito provvedi a cancellarli perché potrebbe trattarsi di indicazioni convenzionali per i malintenzionati.

D: Quali precauzioni da usare quando ci si assenta, ad esempio, per una vacanza ?

R:

- Quando sei in luoghi pubblici (bar, uffici pubblici) dove gli estranei possono ascoltare evita di dare informazioni sui tuoi spostamenti.
- Non lasciare messaggi appesi alla porta di casa. Se sei iscritto a qualche social network evita di divulgare informazioni circa i tuoi spostamenti sia quotidiani che vacanzieri o per quanto tempo rimarrai lontano da casa ed evita di postare foto che riproducano l'interno dell'abitazione o alcuni

particolari di valore che la rendano un obiettivo appetibile per i malfattori.

- In caso di assenze prolungate una precauzione è programma la radiosveglia in casa perché ogni tanto suoni, così da far credere che ci sia sempre qualcuno in casa.
- Posiziona i contatori dell'energia elettrica in vani non accessibili ad estranei (quelli nuovi hanno due spie luminose che segnalano il mancato consumo elettrico per oltre 20 minuti, informando i potenziali malfattori dell'assenza dalla propria abitazione).

D: E quando siamo in strada?

R:

- Portare un telefono cellulare per le emergenze, avendo cura che la batteria sia carica.
- Tenere la borsa chiusa, vicino al corpo, con la chiusura della zip davanti; se vieni scippato, lascia la presa, altrimenti potresti essere trascinato a terra riportando anche ferite.
- Non mettere in evidenza oggetti preziosi che potrebbero essere strappati dai potenziali rapinatori.
- Se ti senti seguito da qualcuno attira l'attenzione delle Forze dell'Ordine che passano in pattuglia o camminano, oppure dirigiti verso la caserma o ufficio più vicino, oppure chiedi aiuto a qualche

passante o entra in un bar, negozio o altro luogo affollato.

D: Nei luoghi affollati?

R:

- Non tenere il portafogli nella tasca posteriore dei pantaloni o in borse che si aprono con facilità.
- Fai attenzione alle persone che ti spingono o ti premono.
- Diffida, anche se mostra modi gentili, di chi ti avvicina con una scusa come chiederti l'ora o farsi cambiare delle banconote.

D: E per quanto riguarda l'auto?

R:

- Non lasciare mai aperte le portiere, e inserire l'antifurto.
- Non lasciare mai le chiavi dell'auto inserite nel quadro di accensione, anche durante le brevi soste.
- Evitare di lasciare incustoditi e ben in vista oggetti di valore (borse, PC, monete) e fare attenzione anche nello spostare tali oggetti dall'abitacolo al bagagliaio perché tale manovra potrebbe attrarre l'attenzione di qualche malintenzionato.
- Chiudi portiere e finestrini quando sei fermo (al semaforo, agli incroci o nei parcheggi) e fai

attenzione agli estranei vicini alla tua auto perché potrebbero tentare di aprire la portiera impedendone la chiusura automatica.

- Non far salire persone estranee.
- Controlla manualmente che le portiere siano chiuse, poiché vi sono attrezzature che consentono di intercettare le frequenze dei telecomandi e bloccare la chiusura automatica delle portiere.
- Parcheggia, se possibile, in luoghi illuminati o vicini a telecamere e durante le soste nelle aree di servizio lascia l'auto bene in vista.
- Non affidare a posteggiatori improvvisati e non autorizzati le chiavi dell'auto.
- Tieni sempre d'occhio l'auto durante le soste di carico e scarico di merce o bagagli.

D: E la bicicletta?

R: Assicura la bici con una catena solida e quando sei in sella riponi la borsa nel cestello avendo cura di bloccarla con la tracolla al manubrio e di non portarla mai in spalla.

Interviste di:
Gabriele Parenti
FAP ACLI Firenze

Si ringraziano:

Dott.ssa Eva Claudia Cosentino
*Primo Dirigente della Polizia di Stato,
dirigente del Centro Operativo
per la Sicurezza Cibernetica (COSC) Toscana*

Cap. Alessandra Giardino
*Capitano dei Carabinieri
Comandante della Compagnia di Pontassieve*

Avv. Francesco Parenti
Foro di Firenze

Dott. Marco Stagi
*Comandante della Polizia Locale
del Comune di Pontassieve (FI)*

FAP Acli Firenze online

Il nostro sito e canali social:

Sito: fapaclifirenze.it

Facebook: www.facebook.com/100081863481506

Canale Youtube: www.youtube.com/@FAPACLIFIRENZE



facebook



You Tube

