QUESTURA DI ROMA

Campagna sicurezza per gli anziani

Alcuni consigli utili per difendersi dai malintenzionati

Se ti senti minacciato o vittima di un reato, chiama subito l'uno uno due

Emergenza 112

E-mail: urp.quest.rm@pecps.poliziadistato.it - upgsp.quest.rm@pecps.poliziadistato.it

CONTENUTI

INFORMARE: INSIEME PER UNA SICUREZZA CONDIVISA!

La solitudine costituisce terreno fertile per le truffe e i raggiri a danno non solo degli anziani ma anche di persone semplicemente distratte in altre attività. Spesso coloro che sono vittime di truffa riferiscono emozioni e sentimenti di paura e vergogna che scaturiscono dagli episodi di cui sono tristemente protagonisti : in quei momenti, infatti, ci si sente fragili, soli, addirittura in colpa per essere caduti nell'inganno, un disagio che si aggiunge al furto o alla truffa subita . In un percorso informativo di "antitruffa e autoprotezione" vengono trattati, da un lato argomenti di natura teorica, incentrati sulla prevenzione e sull'informazione relativa a truffe e furti, con un approfondimento sul tema della componente psicologica, dall'altro si affronta il tema dell'autoprotezione. Fornendo una serie di informazioni preventive a coloro che rappresentano le vittime prescelte dei truffatori, si intende perseguire una prospettiva di prossimità. La polizia è sempre in prima linea nell'attività di contrasto al fenomeno delle truffe nei confronti delle persone "deboli". Si tratta di reati molto odiosi che comportano, per chi li subisce, non solo un danno economico ma anche e soprattutto psicologico, con ripercussioni sullo stile e sulla qualità di vita delle vittime.

Per questo motivo la Polizia di Stato ha raggiunto la consapevolezza che non è sufficiente intervenire quando il reato è già stato commesso, ma è necessario agire prima, con efficace attività di prevenzione, volta a sensibilizzare sul tema della sicurezza, per far conoscere a tutti quali sono i pericoli in cui possono imbattersi, poiché, solo una corretta informazione può scongiurare questa tipologia di reati. Ad ogni modo bisogna tenere comunque ben presente che la Polizia di Stato e le altre Forze dell'Ordine sono sempre al fianco dei cittadini e che basta una semplice telefonata al Numero Unico di Emergenza 112 per un intervento immediato. Le campagne di sensibilizzazione,portate avanti negli ultimi anni, hanno prodotto due effetti positivi: il primo è che si è sempre più informati riguardo ai raggiri di cui si può rimanere vittime e, quindi, sempre più spesso, si riesce a sventare le truffe; il secondo consiste in un' accresciuta consapevolezza del fenomeno e della sua gravità che ha gravità che ha determinato un aumento delle denunce e una riduzione dei fenomeni sommersi.

1. LE FORZE DELL'ORDINE

Polizia di Stato

Carabinieri

Guardia di Finanza

Polizia Municipale

1. Operano di norma in coppia, in divisa e in vetture di servizio.
2. La Polizia di Stato e le altre forze di polizia possono anche svolgere servizio di vigilanza e prevenzione in motocicletta, a cavallo o a piedi, come nel caso dei "poliziotti o dei carabinieri di quartiere" e dei "vigili di prossimità".
3. Agiscono in borghese soltanto in determinate zone e per operazioni specifiche, e sono sempre muniti di tessera e placca di riconoscimento.

Prima di decidere se aprire o meno la propria porta di casa a chi si presenta come rappresentante delle Forze dell'Ordine, è opportuno:

- controllare se in strada è parcheggiata la vettura di servizio;
- capire bene il motivo della visita;
- controllare con cura il tesserino e la placca di riconoscimento;
- osservare, per quanto possibile, i particolari della divisa e degli accessori.

Eventuali malintenzionati potrebbero utilizzare alcune scuse per entrare all'interno della nostra abitazione, ad esempio:

- controllare che il nostro appartamento non sia stato visitato dai ladri, come successo in case vicine;
- ricercare eventuali ladri che si aggirino nelle vicinanze o perché visti entrare nell'androne;
- verificare le banconote tenute in casa o prelevate in banca.

2. I TRUFFATORI COMPORTAMENTI E PROFILI

1. I truffatori possono essere uomini o donne, anche anziani (soprattutto chi si occupa di informare o controllare le spalle ai truffatori).
2. Se operano in borghese, generalmente vestono in maniera elegante. Se indossano delle finte divise, presentano incompletezze e contraffazioni facilmente individuabili. In entrambi i casi, possono esibire finti tesserini di riconoscimento e portare guanti.
3. Di norma, i truffatori usano modi gentili ma decisi, tendono ad essere fini parlatori, si mostrano colti ed esperti, e spesso cercano di disorientare la vittima con un fiume di parole.
4. Potrebbero conoscere il vostro nome e cognome, e fingono, con frasi semplici e brevi, di conoscere figli, mariti, mogli o altri parenti.
5. Possono operare da soli, ma più spesso con uno o più complici per dividersi i compiti.
6. Chi interviene per offrire "aiuto" alla vittima può essere un loro complice.

Spesso nei confronti di donne sole: tendono a presentarsi con profili standard uomini di mezza età, bianchi, solitamente europei,professionisti di successo (ingegnere, architetti e consulenti sono i più gettonati), spesso vedovi con bambini. Raccontano di avere una vita sentimentale triste e alla ricerca di una partner seria e affidabile. In breve tempo diventerà una presenza costante, alla continua ricerca di un rapporto, diventerà una consolazione alle fatiche e alle tristezze e una spalla a cui appoggiarsi. Farà sentire la donna, amata e speciale, fino a rendere la vittima dipendente.

3. SICUREZZA [IN CASA]

ENTI SOCIO-ASSISTENZIALI: INPS, INAIL, ASL

Gli enti socio-assistenziali come l' INPS o l'INAIL non hanno personale operativo che faccia telefonate o visite a domicilio a titolo di prevenzione, accertamento o per ragioni amministrative.

Lo stesso discorso vale per le ASL, con la sola eccezione delle visite specialistiche domiciliari, che però vengono richieste dal medico di base, concordate con l'ufficio competente e preannunciate in modo inequivocabile al paziente.

Non aprite mai la porta e non date ascolto, quindi, ad eventuali sconosciuti che si spacciano per funzionari o ispettori dell'INPS o della propria ASL per:

» accertamenti o conferme di esenzioni del ticket sanitario;

» annunci di rimborsi o di arretrati, spesso presentandovi una finta pratica che richiede il versamento immediato di somme di denaro e la conclusione della pratica presso uno sportello dell' ente;

» controlli di documenti;

» pacchi regalo;

» offerte dei più disparati servizi a fronte di un compenso;

» proposte di vendita di apparecchi medicali.

Nel caso in cui aveste prenotato una visita specialistica a domicilio, fate attenzione se il personale si presenta in un giorno e in un'ora differente da quelli concordati in sede di prenotazione con l'ASL o con il centro medico.

AZIENDE DI SERVIZI: GAS, ENERGIA, ELETTRICA, ACQUA, TELEFONO, RIFIUTI

Nessuna azienda di fornitura di servizi manda funzionari a casa degli utenti per riscuotere l'importo di bollette, per controllarle o per eseguire rimborsi. Le visite dei tecnici vengono comunicate all'utente specificando l'ora e il giorno della visita, oltre ai motivi dell'intervento e le modalità in cui avverrà.

Nel caso si dovesse ricevere una visita sospetta, è meglio invitare il presunto tecnico a ripresentarsi con il portiere o con l'amministratore, annunciando l'imminente arrivo di un parente.

L'importante è non aprire la porta, neppure per controllare il tesserino di riconoscimento mostrato dal presunto tecnico.

Una delle truffe più diffuse è quella del finto amico di famiglia che dice di aver preso accordi con un parente per la consegna o la riparazione di un oggetto e chiede di anticipare il denaro.

SERVIZI BANCARI

Le banche offrono servizi soltanto presso gli sportelli, per corrispondenza, con carte di credito o su Internet. È bene diffidare sempre, quindi, da chi si presenta a casa nostra per un problema legato ai codici personali o ai dati della carta di credito, potrebbe essere un malintenzionato.

Sono truffatori tutti gli sconosciuti che dichiarano di essere incaricati:

- del controllo dei numeri di serie o della sostituzione di banconote in nostro possesso;
- del cambio delle vecchie lire in euro;
- dell' offerta di servizi bancari gratuiti, come le cassette di sicurezza.

Posta e servizi postali

La corrispondenza è lasciata sempre nella buca delle lettere. Le raccomandate e i pacchi sono consegnati sul portone o nell'androne. Se nel nostro palazzo non lavora un portiere e non conosciamo il postino, chi ci citofonerà per consegnarci qualcosa direttamente sulla porta di casa potrebbe essere un malintenzionato.

Parrocchie e Associazioni Religiose

L'attività della parrocchia e la beneficenza vengono usate spesso come scusa da chi vuole entrare in casa nostra con cattive intenzioni. È bene sapere, quindi, che le parrocchie e le associazioni a scopo benefico:

- lasciano lettere nella buca della posta;
- lasciano avvisi e manifesti nell'androne del palazzo;
- non inviano volontari a casa.

Se ti senti minacciato o vittima di una truffa

chiama subito il 112

dove è presente

altrimenti il 113

Gli operatori di: INPS, Poste, Banca, non vengono a casa!

FINTO AVVOCATO

Ricevete una telefonata da un signore dai modi gentili che si presenta come un avvocato. Vi dice che vostro figlio o nipote è responsabile di un incidente, addirittura vuole passarveli al telefono, ma la chiamata è molto disturbata. Ovviamente non è un vostro parente ma è facile cadere in errore perché la notizia dell'incidente vi ha destabilizzato emotivamente. Il truffatore vi dice inoltre che per risolvere immediatamente il problema e non avere guai con la giustizia ha bisogno subito di soldi in contanti per sistemare tutto. Questo sedicente avvocato vi dice anche che vi manderà immediatamente un suo incaricato per ritirarli da voi. Non è vero, è una truffa. Non fatevi imbrogliare e chiamate subito un conoscente che vi può mettere in contatto con i vostri veri familiari. Se non avete nessuno chiamate le forze dell'ordine.

Il truffatore vi dice che per risolvere immediatamente il problema e non avere guai con la giustizia ha bisogno subito di soldi in contanti per sistemare tutto chiama subito il 112

FALSA BENEFICENZA

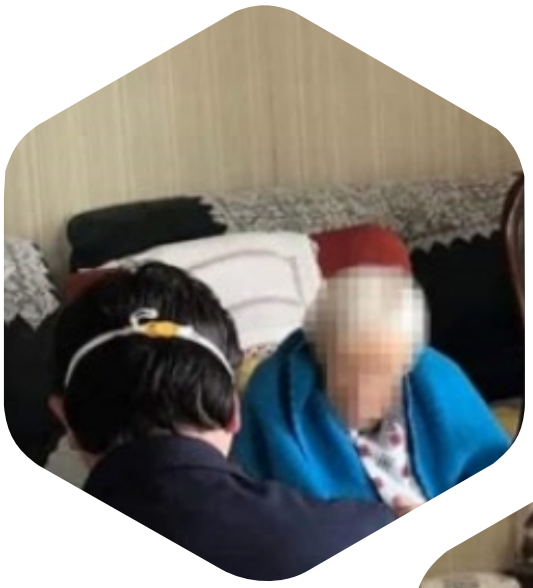
Un signore ben vestito, 50/60 anni circa, a volte con accento straniero, si finge un medico o un rappresentante di una casa farmaceutica alla ricerca di un deposito per effettuare una donazione di medicinali a scopo di beneficenza. Ferma un signore per strada, normalmente in quartieri borghesi, chiedendo informazioni su questo deposito: il signore ovviamente non sa niente Passa un'altra persona, il complice, che fa finta di sapere dove sia il deposito ma dice che è stato chiuso. A quel punto l'unico modo per fare la donazione è solo tramite un notaio ma serve un anticipo in denaro che ovviamente dice di non avere con sé. L'anziana vittima si convince che può contribuire alla beneficenza se fornisce il denaro che serve per il notaio, e come ringraziamento le sarà riconosciuto un compenso in denaro. La vittima viene accompagnata in banca a ritirare una cifra che può essere anche di qualche migliaio di euro e poi viene fatta salire sull'auto per andare dal notaio. Durante il tragitto i truffatori "si ricordano" che sicuramente servirà una marca da bollo. Si fermano davanti a un tabaccaio e chiedono alla vittima cortesemente di andare a comprarla. Appena il truffato scende,naturalmente fuggono.

La beneficenza si effettua solo tramite canali ufficiali e non per strada!!!

FALSA EREDITA'

La stessa procedura della falsa beneficenza è utilizzata anche per la truffa delle eredità da consegnare. Un signore si spaccia per qualcuno in cerca di un vecchio amico a cui dovrebbe consegnare del denaro relativo a un'eredità. Ferma una persona anziana per chiedere informazioni su quel fantomatico amico ma ovviamente nessuno lo conosce, finché un passante, complice del truffatore, si ferma e dice che quella persona è morta.
L'unica soluzione è il notaio ma serve l'anticipo.
E l'epilogo è sempre la fuga dopo aver fatto allontanare la vittima con un pretesto.

Per ricevere un'eredità occorre un notaio che nel suo studio vi comunica tutte le informazioni necessarie. Diffidate sempre dagli estranei che vi chiedono soldi per strada!!



4. SICUREZZA [IN STRADA]

In generale i truffatori scelgono la propria vittima quando è:

- meno attenta, perché sta osservando prodotti, prezzi o sta chiacchierando;
- in affanno, perché sta maneggiando soldi oppure sta controllando i risultati di un visita medica o di esami clinici;
- distratta con un sotterfugio, come una spinta o una moneta lanciata a terra;
- in un momento di relax, perché seduta al tavolo di un bar, ai giardini pubblici o in qualsiasi luogo dove l'incontro può diventare tanto cordiale da indurre la vittima ad invitare il malvivente a casa.

BANCOMAT E SERVIZI ALLO SPORTELLO

Recarsi in banca o all'ufficio postale per prelevare soldi contanti è un'operazione sempre più comune. Per renderla sicura basta prendere alcuni piccoli accorgimenti accorgimenti.

In particolare, all'uscita della banca o dell'ufficio postale, è opportuno:

- non distrarsi;
- non fermarsi con sconosciuti;
- camminare sul lato più sicuro del marciapiede, quello più lontano dalla strada così da evitare di prestare la borsa a possibili scippi.

Fuori dalle mura domestiche, le truffe ai danni degli anziani possono avvenire in diversi luoghi. I malintenzionati sfruttano la confusione dei posti affollati, come i mezzi pubblici, i mercati e i luoghi di ritrovo in generale, inclusi cinema, chiese o feste di paese.

La truffa dello specchietto è una di quelle più diffuse, dove il truffatore fa credere all'automobilista che ha urtato con la sua macchina il suo specchietto retrovisore, facendosi così risarcire.

Mentre si carica la spesa in auto all'interno del parcheggio del supermercato, si può essere vittima di furto della borsa, mentre un complice distrae la vittima facendo cadere le monete.

In questo caso è opportuno lasciare la presa della borsa prima di essere trascinati a terra, riportando ferite anche gravi.

Una volta prelevato il denaro, uno dei trucchi più usati dai malfattori è quello di **segnare** gli abiti della persona che ha appena effettuato l'operazione e che, quindi, ha somme di denaro con sé, senza che questo se ne accorga.

Per farlo, I truffatori possono appendere ai vestiti della vittima il cosiddetto **filo di banca,** oppure **segnare** gli abiti della persona con un gesso o altri segni di riconoscibilità da parte di un complice, che a quel punto seguirà la la vittima. Se il truffatore dovesse arrivare fino alla porta di casa, senza che il cittadino se ne accorga, i malviventi potrebbero:

- fingersi dipendenti della banca in cui è stato fatto il prelievo, inventando possibili modi per controllare le banconote, o cambiarle, ecc;
- convincere la vittima a recarsi in banca o alla posta per prelevare altro denaro.

Per ridurre questo tipo di rischio, è consigliabile richiedere l'accredito **su conto corrente bancario o postale.**

Durante il tragitto di andata e ritorno dalla banca o dall'ufficio postale:

. Con i soldi in tasca, non fermatevi con sconosciuti e non fatevi distrarre.

. Dividete il denaro in più tasche, possibilmente interne all'abito e non fate notare quanto avete prelevato.

. Ricordatevi che nessun cassiere di banca o di ufficio postale vi insegue per strada per rilevare un errore nel conteggio di denaro che vi ha consegnato.

. Evitate strade solitarie, specialmente la sera e non sostate in luoghi appartati.

FALSE PIETRE PREZIOSE

Una delle truffe più ricorrenti. Un signore con aspetto rassicurante e in genere di mezz'età si finge straniero e dice che per un'urgenza deve raggiungere il Paese d'origine ma non ha disponibilità di soldi liquidi per il viaggio.
Generalmente ferma una signora per strada e cerca di venderle un anello o delle pietre preziose che a suo dire avrebbero un valore di alcune migliaia di euro ma, vista la situazione urgente, è disponibile a venderle alla signora a molto meno. In quel momento passa un altro signore ben vestito che dice di essere un gioielliere e mostra tanto di lente per controllare le pietre. Breve controllo e subito si offre di comprarle a **5 mila euro**. A quel punto lo straniero mostra simpatia per la vittima e insiste che sia lei a comprarle. **E spesso riesce a convincerla facendosi dare 'solo' 2/3 mila euro.**

I gioiellieri non acquistano per strada pietre preziose!

NON FIDATEVI!!!

5. SICUREZZA [INTERNET]

Evitare pericoli presenti in Rete è semplice, basta adottare qualche piccolo accorgimento.

1. Scegliamo una password complessa, che contenga numeri, lettere e, possibilmente, anche caratteri maiuscoli e minuscoli.
2. Non mettere a disposizione i propri dati di accesso a social network, caselle postali, ecc.
3. Non aprire mai le email e gli allegati che arrivano da sconosciuti.
4. Non facciamoci ingannare da finti annunci di vincite in denaro o di offerte di lavoro.
5. Un computer che non ha un programma antivirus aggiornato è più vulnerabile.
6. Se il nostro computer ha una videocamera integrata, è opportuno controllare che si accenda al nostro comando e che non sia sempre attiva.

Sempre più spesso gli anziani usano internet, incuriositi dall'utilizzo che ne fanno nipoti e figli.
La rete offre infinite possibilità ma nasconde anche dei rischi, dietro a email e pagine internet, infatti, possono nascondersi dei malintenzionati.

GLOSSARIO

ADWARE: Particolare versione di spyware atto a monitorare informazioni personali o sensibili a fini pubblicitari.

ANTISPAM: Programma o tecnologia che impedisce, o quantomeno limita, la ricezione di posta indesiderata nella propria casella di posta in entrata.

ANTISPYWARE: Il software antispyware protegge il computer da popup pubblicitari, lentezza e minacce alla sicurezza dovute a spyware e altro software indesiderato.

ANTIVIRUS: Programma che individua, previene e rimuove programmi dannosi, come virus e worm. Affinché sia efficace deve essere costantemente aggiornato.

ATTIVAZIONE: Procedura indispensabile, connessa all'installazione di molti software per attestarne la genuinità.

BACKDOOR: Accesso abusivo a un sistema informatico. Di solito una backdoor viene inserita dagli stessi programmatori del sistema per poter effettuare accessi di emergenza, ma a volte gli hacker riescono a individuarle sfruttandole a proprio vantaggio.

BACKUP: Operazione che consiste nel salvare periodicamente i dati memorizzati sul disco fisso del PC.

BODY SHAMING (vergogna del corpo): è la tendenza a commentare sui social network, in modo negativo, la forma fisica delle persone, in particolare delle donne, con lo scopo di far vergognare la 'vittima' del proprio corpo, con il pericolo di spingerla verso un comportamento alimentare scorretto.

"I sistemi informatici custodiscono dati sempre più preziosi e la loro violazione arreca ormai danni notevoli anche ad aziende ed istituzioni pubbliche e governative.

BOT: Il termine bot è un'abbreviazione di 'robot'. Pirati informatici li usano per trasformare il tuo computer in un dispositivo in grado di effettuare automaticamente operazioni su internet a tua insaputa.

CAT FISHING (pesce gatto): in inglese vuol dire pesce gatto e in gergo urbano vengono descritte con questo termine coloro che sui social network fingono di essere qualcun altro solitamente per intrecciare delle storie amorose virtuali.

CHAT: Significa 'chiacchierare' e indica le conversazioni scritte in tempo reale che si possono fare in rete con altri utenti tramite appositi programmi, per esempio Messenger e Skype.

CLOUD: Il termine inglese cloud computing indica un insieme di tecnologie che permettono di memorizzare ed elaborare dati grazie all'utilizzo di risorse hardware e software distribuite e virtualizzate in rete. SkyDrive e le Office Web Apps sono un esempio di servizio cloud offerto gratuitamente da Microsoft.

CONTROLLO ACTIVEX: I controlli ActiveX sono piccoli programmi che vengono utilizzati su internet. Nella maggior parte dei casi sono utili, per esempio per l'installazione di aggiornamenti di sicurezza, ma se usati illegalmente possono effettuare attività senza il tuo controllo.

COOKIE: I Cookie sono piccoli file che i siti web salvano sul tuo disco rigido alla tua prima visita. Il loro compito è quello di ricordare i tuoi dati quando ritorni a visitare un sito. Generalmente i cookie non sono dannosi, ma se usati in maniera fraudolenta possono sottrarre informazioni a tua insaputa.

COPYRIGHT: E' il diritto di autore che stabilisce la proprietà intellettuale di un'opera.

CRACCARE: neologismo gergale da 'to crack', 'spezzare'. Si intende il superamento delle protezioni di un programma o di un sistema informatico.

Social Network consiste nella realizzazione di un gruppo di individui connessi tra loro da diversi legami ed interessi attraverso internet.

CRACK: Un sistema, generalmente software, in grado di eliminare le protezioni che vengono normalmente applicate ai programmi per evitare che vengano duplicati e installati illecitamente.
L'utilizzo dei crack è illegale.
CRACKER: Declinazione negativa dell'hacker.
Quest'ultimo generalmente viola i sistemi informatici solo per metterli alla prova, mentre il cracker lo fa con l'obiettivo di sottrarre i dati, danneggiare i sistemi o sottrarre denaro, per esempio da un conto corrente online.
CREAZIONE DI SITI WEB: Per ridicolizzare o prendere in giro qualcuno.
CYBERBASHING (bastonata): è la forma di cyberbullismo più famosa perché oggetto di cronaca recente. Inizia nella vita reale dove la vittima viene aggredita o molestata mentre altri riprendono la scena con la telecamera del cellulare, poi la violenza continua postando le immagini su internet condividendole commentandole o votandole come video divertente addirittura consigliato in rete.
CYBERBULLISMO: Termine che identifica attività di bullismo perpetrate tramite internet.
CYBERPEDOFILIA: Il pedofilo telematico è un individuo estremamente pericoloso perché spesso è difficile da individuare. Tipicamente cerca di instaurare un clima di fiducia e amicizia fingendosi coetaneo dei bambini e cercando di agire quando il minore non è controllato da persone adulte.
CYBERSTALKING (persecuzione online): invio ripetuto di messaggi denigratori, incluse minacce, miranti ad includere paura.
DENIGRATION (denigrazione): è una forma di cyberbullismo che ha lo scopo di ledere la reputazione della vittima denigrandola pubblicando materiale come video o foto o anche semplicemente parlandone male.

Cyber-Bullismo è una forma di bullismo realizzata attraverso internet.

DIALER: E' uno speciale programma auto-eseguibile che altera i parametri della connessione a internet.
DISCLAIMER: Significa 'esonero di responsabilità'.
DRM: Acronimo di Digital Right Management, standard ideato da Microsoft sulla gestione dei diritti relativo alle opere digitali protette da copyright.
CYBERBULLISMO: Termine che identifica attività di bullismo perpetrate tramite internet.
EXCLUSION (esclusione): Esclusione di qualcuno da un gruppo online.
EXPOURE (rivelazione): Rivelazione di informazioni o particolari che riguardano la vita privata di qualcuno senza il suo consenso.
FAKE: Identifica un falso.
FILTRO SMART SCREEN: Il filtro Smart Screen è una funzionalità di Internet Explorer 9 e 8 che ti aiuta a evitare le minacce di ingegneria sociale.
FIREWALL: Un firewall è un programma software o un componente hardware che permette di respingere gli attacchi di hacker.
FIRMA DIGITALE: Procedura che garantisce l'integrità e l'autenticità di un documento informatico.
FLAME: Identifica un attacco o reazione aggressiva verbale nei confronti di un utente.
FLAMING (in fiamme): Litigi on line nei quali si fa uso di un linguaggio violento e volgare che possono coinvolgere una singola persona o un gruppo di amici.
FURTO DI INDENTITA': Il furto di identità è un qualsiasi tipo di frode che porta alla perdita di dati personali, come password, nomi utenti,dati bancari o numeri di carte di credito. La forma più diffusa è il phishing, ovvero la frode perpetrata tramite email.
FURTO DI PASSWORD: La password viene decriptata allo scopo di chattare fingendosi la vittima per insultare amici, sconosciuti o inserire commenti razzisti o a sfondo sessuale.

Il furto di identità avviene anche attraverso la rete online soprattutto in occasione di acquisti.

HACKER: Nella sua forma più pura si può considerare una sorta di studioso dei sistemi informatici, che tenta di violare per saggiarne i limiti e la sicurezza senza provocare danni. Purtroppo sempre più spesso gli hacker diventano cracker, ovvero persone che lo fanno a scopo di lucro, per sottrarre dati o mettere fuori uso i sistemi informatici.
HARASSMENT (molestia): Spedizione ossessiva e ripetuta di messaggi denigratori mirati a ferire un bersaglio preciso.
HOAX (FINTE MAIL): Un fenomeno legato al Phishing e al furto di indentità. Si tratta di finte mail, per esempio provenienti da istituti bancari o altri organismi, il cui unico scopo è sottrarre informazioni personali.
HTTPS: L'utilizzo del protocollo HTTPS (Hypertext Transfer Protocol Secure) consente di proteggere le informazioni inviate in Internet.
ICRA: Internet Contant Rating Association. Un'associazione internazionale senza fini di lucro nata per difendere e aiutare la navigazione dei minori in rete.
IMPERSONATION (imitazione): si tratta di un vero e proprio furto di identità e integra un comportamento penalmente rilevante.
NEKNOMINATION (prossima nomina):Una sorta di catena di Sant'Antonio nella quale i ragazzi vengono nominati ovvero chiamati ad eseguire una vera e propria prova di coraggio.
PERSECUZIONE VIA CHAT: Si tratta di offese, insulti o arbitrarie esclusioni dai gruppi o dalle chat di WhatsApp.
PHARMING: Tecnica che permette di sfruttare a proprio vantaggio la vulnerabilità di server controllando il dominio di un sito e utilizzandolo per redigere i tratti su un altro sito.

Le attività finalizzate a intimorire e minacciare possono essere effettuate con molta efficacia anche sui Social.

NETIQUETTE: Insieme di regole che disciplinano il comportamento di un utente in internet.
NETIZEN: Il termine significa 'cittadino della Rete'.
NEWBIE: Neologismo gergale che indica un nuovo utente della rete, un navigatore alle prime armi.
NICKNAME: Quando non si vuole usare il proprio nome in rete, si può scegliersi un soprannome.
PEER-TO-PEER: Architettura di rete nella quale tutti i computer funzionano sia come client che come server.
INPRIVATE BROWSING: Tecnologia che consente di evitare che la cronologia delle esplorazioni, i file internet temporanei, i dati dei moduli, i cookie nonché i nomi utente e le password vengano mantenuti nel browser.
MALWARE: Con questo termine si identifica un software che viene installato senza il tuo consenso.
MASQUERADE (mascherata): Sostituzione di persona che ha lo scopo di spedire messaggi a nome altrui.
MICROSOFT SECURITY ESSENTIAL: Microsoft Security Essential è un software antimalware gratuito per il tuo computer.
INTERNET POLLING (elezioni on line): veri e propri sondaggi on line in cui le vittime sono classificate in base ad elementi denigratori.
LOGIN: Procedura di accesso a un computer, a un programma o a un servizio, generalmente legata all' inserimento di un username e di una password.
LURKER: Nelle attività in rete indica chi osserva senza prendere parte attiva.
PARENTAL CONTROL: Un filtro che permette di bloccare la visione dei contenuti non adatti ai bambini o a persone particolarmente sensibili.
PHISHING: Il phishing è un furto di identità on line.
POP-UP: Il termine significa 'saltar su' e indica le finestre che si aprono nel browser in modo automatico, di solito a scopi pubblicitari.

Prima di inserire i dati personali all'interno di finestre 'di dialogo' su internet è opportuno chiedere informazioni.

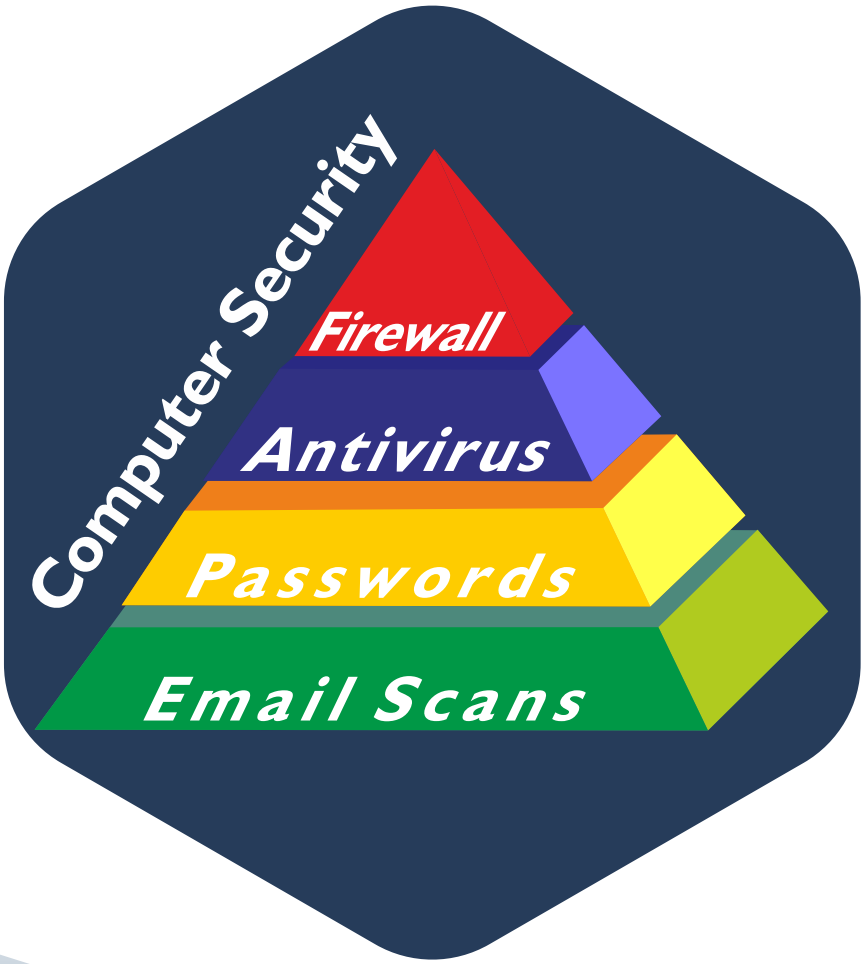
PROXY SERVER: Un server che si interpone tra i computer di chi naviga il web.
PUT DOWN (denigrare): Ovvero denigrare qualcuno attraverso email, sms, post inviati ad un blog, ovvero un gruppo di persone.
RIPPER: E' così definito un programma che acquisisce i dati da CD musicale DVD video.
SEXTING (pubblicare sesso): Si può definire sexting, l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite, inerenti la sessualità.
SPAM: Lo spam è qualsiasi tipo di comunicazione online indesiderata.
SPYWARE: Spyware è un termine che descrive un software che si installa sul computer senza il tuo consenso.
TEXT WAR (guerra di messaggi): Un gruppo si coalizza contro un singolo inviando moltissimi sms dal numero di telefono della vittima alla quale vengono addebitate le fatture telefoniche.
TRACKING PROTECTION LIST: La TPL o Protezione da monitoraggio, permette di scegliere i siti autorizzati a ricevere le informazioni che riguardano la navigazione da parte dell'utente e di controllare la propria privacy durante la navigazione.
TRICKERY (inganno): si ricevono confidenze o racconti, anche imbarazzanti, dalla vittima fingendosi suoi amici per poi condividerli con gruppi di altre persone.
TROJAN: E' un software che nasconde al suo interno un virus. Installando ed eseguendo il programma che contiene il Trojan, l'utente innesca il virus.
VIRUS: I virus informatici sono softwareprogettati per diffondersi da un computer all'altro e interferire con il funzionamento della macchina.
WAREZ: Neologismo usato per individuare software scaricabili abusivamente e illegalmente dalla rete.

Lo strumento della rete digitale è meraviglioso ed efficace se utilizzato correttamente.

WEP:Acronimo di Wired Equivalent Privacy, un sistema di crittografia che si basa su una chiave pubblica. Serve per rendere più sicure le comunicazioni wireless.

WARNING WARS (guerre di allarmi): Vere e proprie guerre di segnalazione condotte sfruttando l'opportunità, offerta da molti provider, di segnalare chi posta sul proprio account commenti inappropriati.

WORM: Il worm è un particolare virus informatico in grado di propagarsi senza la necessità che l'utente inneschi il suo funzionamento compiendo un'operazione.



6. LA RETE SOLIDALE

E' possibile vivere in maniera sicura in casa propria, sui mezzi di trasporto, nei luoghi pubblici, in banca o all'ufficio postale.

Bastano pochi accorgimenti e, soprattutto, la rete di solidarietà che nasce nel contesto in cui viviamo.

Il nostro vicino, un amico che può aiutarci nella gestione del quotidiano e le persone di nostra fiducia sono parte integrante della nostra vita, sono loro che dobbiamo tenere in considerazione, anche nei momenti di difficoltà, se siamo in pericolo o se abbiamo subito una truffa.

A prescindere dalla nostra età, ricordiamoci sempre che la migliore prevenzione che si possa adottare è aiutarci l'un l'altro.

Consigli per i parenti:
non lasciate soli i vostri anziani, non aggrediteli e non umiliateli se venite a sapere che sono stati vittime di raggiri, ricordate che hanno bisogno di voi anche se non ve lo chiedono

Consigli per i vicini di casa:
se conoscete qualche anziano che vive da solo nel vostro condominio, fatevi contattare se riceve la visita inaspettata di qualcuno e se è sospetto chiamate la Polizia

Consigli per gli impiegati di sportello:
se un anziano si presenta da voi per una richiesta spropositata di denaro, cercate di capire se c'è qualcuno all'esterno che lo sta raggirando, e cercate di avvertire un parente

7. CONCLUSIONI

In questo opuscolo, breve e di facile lettura, abbiamo voluto raccontare le situazioni che maggiormente espongono gli anziani ai raggiri dei malintenzionati. Attività del quotidiano che vengono percepite con difficoltà, con ansia ed eccessiva preoccupazione, quando basterebbero pochi accorgimenti per viverle in assoluta serenità.
Ricordiamoci sempre che rispondere con un deciso ''mi scusi non ho tempo'' a chi ci telefona, che respingere senza replica lo sconosciuto che citofona inventando scuse e stratagemmi per entrare in casa, che evitare di distrarsi e di farsi distrarre quando si esce dall'ufficio postale o dalla banca, sono tutte regole che ci permettono di tenere lontano da noi eventuali malintenzionati.
In ogni caso, se qualcuno dovesse truffarci, confidiamo sui nostri cari, sugli amici e sui vicini, contattando immediatamente le forze dell'ordine perché è insieme che si costruisce la nostra sicurezza quotidiana.

26-AGO-2019 CORRIERE DELLA SERA da pag. 19

Quotidiano nazionale Direttore: Luciano Fontana Lettori Audipress 04/2019: 275.328

I super detective della polizia contro le truffe agli anziani

Un vademecum anti-raggiri pensato dagli specialisti del Servizio analisi criminale

Il fenomeno
Ogni giorno in Italia 54 persone over 65 denunciano le azioni dei truffatori

Divise e inclusione
La strategia di Gabrielli: dagli aiuti ai disabili, all'ippoterapia con la squadra a cavallo

Il caso

di **Rinaldo Frignani**

ROMA Cinquantaquattro truffe al giorno. In pratica, ogni ora, due persone over 65 rimangono vittime di raggiri. E queste sono solo quelle che poi denunciano il fatto alle forze dell'ordine. Perché sono moltissimi coloro che, invece, per vergogna e paura lasciano perdere. Il fenomeno è tornato a crescere da Nord a Sud, con quasi 20 mila casi nel 2018, rispetto ai poco più di 19 mila dell'anno precedente.

Il 2019, in attesa di dati definitivi, già si annuncia come particolarmente difficile per i più anziani, soprattutto quelli che d'estate sono rimasti da soli in città. E se, stando al dossier del Dipartimento di pubblica sicurezza del ministero dell'Interno, in generale i reati che hanno come vittime gli over 65 sono in diminuzione costante (327.246 nel 2018, -2,7% rispetto al 2017 e -5,1% sul 2016), preoccupa il fatto che fra questi proprio le truffe siano in controtendenza.

Da qui la necessità di avere una strategia di difesa per la categoria sociale più numerosa d'Italia — visto che comprende il 35% della popolazione, la percentuale più alta d'Europa —, ma anche di studiare un sistema di reale inclusione quotidiana di soggetti spesso deboli e indifesi, che porti la polizia a rappresentare lo Stato anche nell'ottica di far sentire meno soli cittadini senza riferimenti e sostegni psicologici ma bisognosi di aiuto.

Gli esempi non mancano. A cominciare dalla storia di Iole e Michele, coppia di anziani coniugi della periferia della Capitale, ai quali mesi fa quattro agenti del Reparto volanti hanno cucinato il pranzo dopo essere intervenuti per soccorrerli in casa. Vicende di umanità quotidiana che spesso danno risultati più profondi, che portano anche a una reazione positiva (e a volte inaspettata) di chi si ritrova vittima di balordi e truffatori. Come la pensionata milanese di 85 anni che ha fatto arrestare chi si spacciava per telefono per il nipote bisognoso di soldi e la 91enne fiorentina che ha smascherato un falso tecnico del gas intenzionato a svaligiarle l'appartamento.

Per alzare il livello di guardia, quest'anno sempre la polizia ha organizzato convegni con l'Anap Confartigianato, Prefetture, Comuni e psicologi durante i quali sono stati analizzati i rischi per la sicurezza degli over 65.: per la prima volta sono stati distribuiti vademecum per difendersi dalle truffe, in casa e fuori, messi a punto addirittura dagli specialisti del Servizio di analisi criminale della Direzione centrale della polizia criminale. Cacciatori di latitanti e serial killer al servizio delle fasce deboli, uno schermo protettivo che non si ferma al classico (anche se meno scontato di quel che si pensi) «non aprite la porta agli sconosciuti», ma che detta alle possibili vittime (e a chi suo malgrado ci è già passato) i tempi del nemico, per anticipare le sue mosse.

Anche questa è strategia di inclusione, voluta dal capo della polizia Franco Gabrielli, al pari di quella studiata per aiutare i più giovani e i disabili. Per questi ultimi, ad esempio, un poliziotto malato di Sla, Gaetano Fuso, ha allestito vicino a Lecce con la collaborazione di polizia e associazioni di volontariato, uno stabilimento balneare (La Terrazza, sulla spiaggia di San Foca a Melendugno). Testimonianza di impegno che si unisce all'ultimo Disability Pride, a piazza del Popolo, a Roma, e all'attività della Squadra a cavallo di Trastevere, più volte a disposizione per sedute di ippoterapia a favore di ragazzi con gravi problemi. Ma inclusione quest'anno significa anche coinvolgere gli studenti delle scuole primarie di cinque regioni e 20 province ai quali, con la collaborazione di Miur e ministero delle Finanze, e prima di sedersi ai banchi, è stato distribuito «Il mio diario», dove si affrontano temi come bullismo e cyberbullismo, educazione stradale e integrazione sociale, rispetto dell'ambiente e degli animali. Come i cani, al centro della campagna anti-abbandono 2019 della polizia, con lo slogan «L'amicizia è una cosa seria». Anche questo un fenomeno in crescita: 955 denunce dal 2017, 352 delle quali proprio d'estate.

NOTE

NOTE

NOTE

N.U.E.
NUMERO UNICO DI EMERGENZA

Progetto grafico, realizzazione e stampa a cura del Centro Stampa dell'U.S.T.L. della Questura di Roma