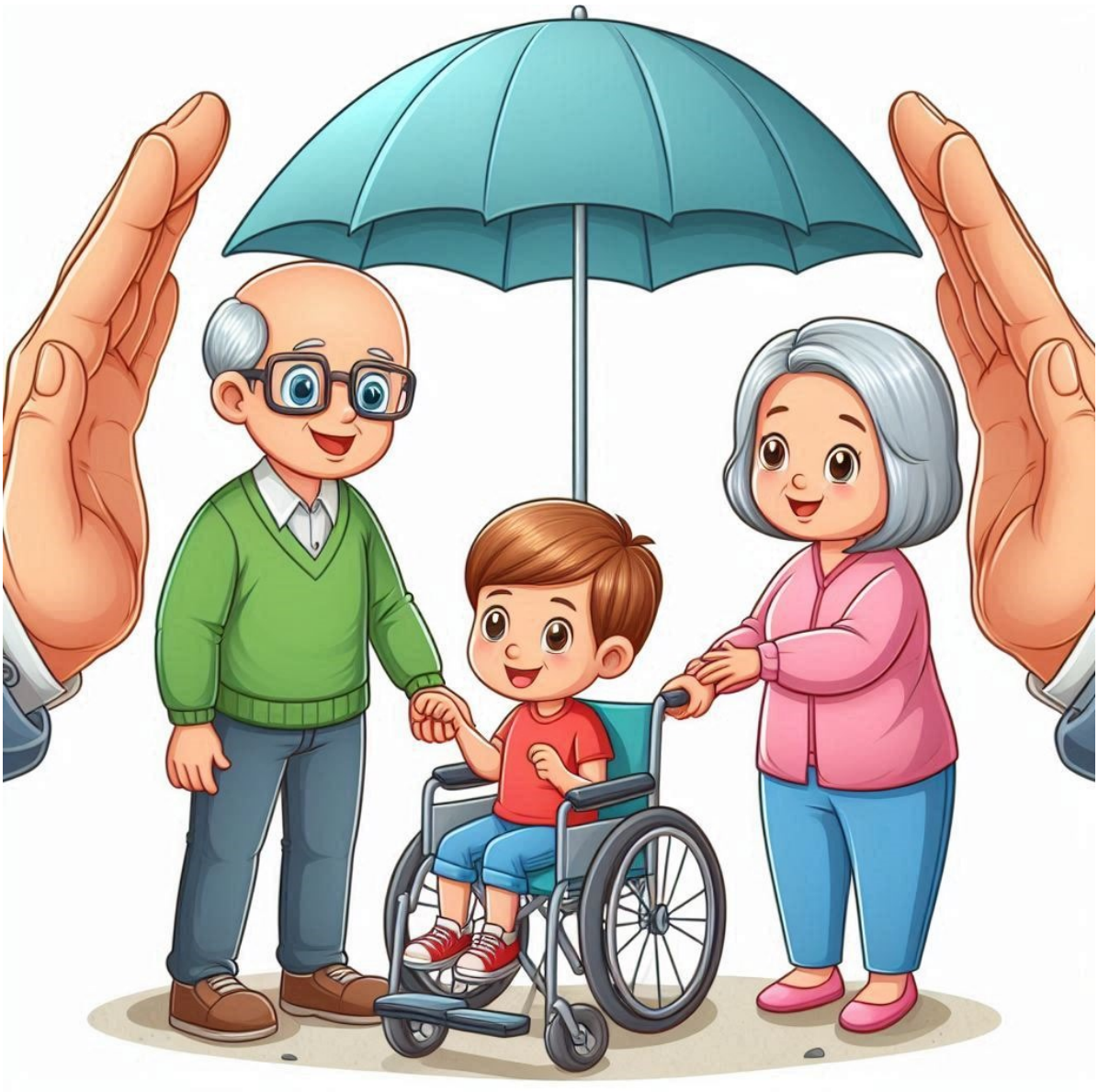
VADEMECUM CONTRO LE TRUFFE

INSIEME SIAMO PIÙ FORTI



INDICE

PREMESSA p. 05

I. **I DESTINATARI** p. 07

II. **I TRUFFATORI** p. 09

III. **A CASA** p. 11

a. I falsi amici p. 14

b. Il finto corriere p. 17

c. Il finto agente assicurativo p. 19

d. Il finto avvocato o alle forze dell'ordine p. 21

e. Come proteggere la casa p. 25

IV. **PER STRADA**

a. Nel parcheggio del supermercato p. 31

b. Vicino alla banca o alla posta p. 33

c. Al parco o per strada

- Una spinta di troppo p. 35
- La truffa dell'abbraccio p. 37
- Il finto malessere p. 39
- Maghi e santoni p. 41

© Cavoli Sergio 2025 – "Vademecum contro le Truffe: Insieme siamo più forti"

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l'autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

- L’inganno della borsa p. 43
- L’inganno del giubbotto p. 45
- L’inganno del finto fruttivendolo p. 47
- La deviazione p. 49
- Il cerchio p. 51
- Due minuti p. 53

V. **IN BICICLETTA** p. 55

VI. **SUI MEZZI PUBBLICI** p. 57

VII. **IN MACCHINA**

- Alla guida p. 59
- In sosta p. 61
- La bottiglietta di plastica p. 63

VIII. **NEI LOCALI PUBBLICI** p. 65

IX. **TRUFFE INFORMATICHE** p. 66

- *Man in the middle* p. 69
- Truffe col *Trading online* p. 71
- *Cryptolocker* p. 73
- *Digital extortion* p. 73
  Truffa romantica p. 75
- *Sex extortion* p. 77
- *The evolution of triple extortion* p. 79

- Consigli per la compravendita di oggetti su Internet p. 81
- La finta eredità p. 83
- Pagamenti PAYPAL p. 83
- Vincite a premi/lotterie p. 83
- *Phishing* p. 85
- *Vishing* p. 87
- *Smishing* p. 87
- *Pharming* p. 87
- *Trojan* p. *89*
- Raccolta Fondi (*Fake Crowdfunding*) p. 91
- L'inganno con il viso di un Nostro familiare p. 93
- Giochi Quiz e Test on-line p. 95
- Truffa del finto lavoro p. 99
- Il finto CUP p. 103
- Lo spid invisibile p. 105
- Il finto Carabiniere/ Poliziotto/Finanziere p. 107
- Borseggiatori con il POS p. 109
- L'assicurazione troppo conveniente p. 111
- La polizza vita sicura p. 113
- **Ricorda sempre** p. 115
- **Ringraziamenti** p. 117
- **Sicurezza degli account online** p. 119

PREMESSA

In queste pagine ho raccolto situazioni purtroppo sempre più diffuse, che espongono gli anziani e le persone vulnerabili ai raggiri di malviventi senza scrupoli.
Si tratta di un fenomeno in costante crescita, una vera emergenza sociale spesso sottovalutata o affrontata con troppa leggerezza.
Mi chiamo Sergio Cavoli e sono un pensionato. Da molti anni mi impegno concretamente nel sostegno alle persone fragili, in particolare a chi, come me, convive con la sclerosi multipla.
Da oltre un anno sono impegnato in una complessa battaglia personale contro un tumore, un'esperienza che ha rafforzato in me il valore della solidarietà, della condivisione e dell'aiuto reciproco.
Da questo percorso è nato il libro *"Passi di Speranza"*, una testimonianza di coraggio e resilienza che racconta come, anche nella prova più dura, sia possibile trasformare la sofferenza in opportunità di crescita e di servizio verso gli altri.
Con lo stesso spirito nasce ora il **Vademecum contro le truffe agli anziani e ai fragili**, uno strumento pratico, chiaro e facilmente consultabile, pensato per essere tenuto in casa e condiviso con chiunque possa averne bisogno.
Il *Vademecum* raccoglie oltre quaranta esempi di tentativi di truffa – reali o verosimili – che colpiscono sempre più spesso anziani e persone fragili. È articolato in tre sezioni principali:
Truffe a casa, Truffe per strada e Truffe informatiche, e si propone di:

- sensibilizzare e informare sulle principali tipologie di truffe oggi in circolazione;
- fornire consigli pratici per riconoscere i segnali di pericolo e reagire con prontezza;
- promuovere una cultura della prevenzione e della sicurezza condivisa, come strumento fondamentale di tutela personale e collettiva.

Con la giusta informazione e qualche semplice accorgimento, tutti possiamo imparare a proteggere noi stessi e le persone che amiamo. Ricordiamoci sempre che **la prevenzione è la nostra migliore difesa.**
E se, nonostante tutto, dovesse capitare di cadere vittima di un raggiro, non bisogna vergognarsi: parlarne con qualcuno di fiducia e rivolgersi tempestivamente alle forze dell'ordine è il primo passo per reagire e tutelarsi.
Solo attraverso la consapevolezza, la collaborazione e la vicinanza reciproca possiamo davvero proteggere chi è più esposto.

Insieme possiamo fare la differenza.

Insieme possiamo affrontare e superare ogni ostacolo.

Insieme possiamo trasformare le difficoltà in forza.

NUMERO UNICO EUROPEO PER LE EMERGENZE



Proteggere i più fragili è un dovere di tutti

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

I. I DESTINATARI

L’aumento preoccupante delle truffe, soprattutto a danno di anziani e persone fragili, ha reso necessario questo vademecum, pensato per fornire indicazioni pratiche utili alla prevenzione.

Chi è più vulnerabile – per età, salute o condizioni di vita – è spesso un bersaglio privilegiato di truffatori e ladri. Molti vivono soli, con limitata mobilità o patologie croniche, e talvolta conservano in casa denaro o oggetti di valore, per sfiducia verso banche o poste. Tutti questi fattori aumentano il rischio di essere raggirati o derubati.

È fondamentale ricordare che la fragilità non è solo anagrafica: riguarda anche la salute, l’isolamento sociale e le difficoltà emotive. Le abitazioni di queste persone diventano obiettivi facili per chi approfitta della loro fiducia o disattenzione anche perché non sempre hanno fiducia .

Prevenire è possibile. In queste pagine troverete consigli semplici e immediati per riconoscere i pericoli, evitare i comportamenti rischiosi e sapere a chi rivolgersi in caso di bisogno.

La sicurezza nasce dalla consapevolezza e dalla collaborazione.

Le Forze di Polizia – Carabinieri, Polizia di Stato, Guardia di Finanza e Vigili del Fuoco – garantiscono ogni giorno il controllo del territorio.

In caso di dubbi o situazioni sospette, chiamiamo sempre il

NUMERO UNICO EUROPEO PER LE EMERGENZE





© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

II. I TRUFFATORI

I truffatori possono assumere diverse forme e operare in vari contesti. Viviamo in una società dove le apparenze possono ingannare, e purtroppo ci sono individui che sfruttano la vulnerabilità per mettere in atto truffe e inganni. In questo vademecum rappresentiamo alcuni dei più comuni:

- truffatori di strada: operano fisicamente, per strada o presentandosi alla tua porta, mettendo in scena situazioni disperate per derubarti o per vendere beni, spesso falsi, a prezzi stracciati;
- truffatori online: sfruttano internet per perpetrare frodi, come il phishing, dove cercano di ottenere informazioni personali fingendo di essere entità affidabili;
- truffatori telefonici: utilizzano chiamate telefoniche per ingannare le persone, talvolta spacciandosi per funzionari di enti pubblici o rappresentanti di aziende.

© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

III. A CASA

NON APRIRE LA PORTA: UN INVITO ALLA VIGILANZA

Negli ultimi anni abbiamo assistito a un preoccupante aumento di truffe perpetrate da individui che si spacciano per membri delle forze dell'ordine o operai autorizzati.

Indossare un’uniforme o presentarsi con un tesserino di riconoscimento può sembrare un segnale di legittimità, ma non è sempre sinonimo di verità. I malintenzionati sono sempre più astuti e abili nel creare falsi documenti e nell’imitare l’aspetto degli agenti o dei professionisti del settore per guadagnare la fiducia delle vittime.

La scusa per entrare in casa può variare: dalla presunta necessità di verificare un'infiltrazione d'acqua a pericoli più gravi come fughe di gas. Una volta dentro, il risultato è quasi sempre lo stesso: furto e depredazione.

I truffatori possono mascherarsi sotto diverse identità:

- Funzionari delle Poste
- Operatori di enti di beneficenza
- Rappresentanti dell'Inps, del Comune o delle aziende di luce, acqua e gas
- Persone che dichiarano di appartenere alle forze dell'ordine.

Sempre cordiali e ben vestiti, cercano di trasmettere un senso di rassicurazione. La loro gentilezza potrebbe però nascondere un intento malevolo.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

Prima di aprire la porta di casa:

1. Non aprire subito la porta: se hai dei dubbi, è sempre meglio mantenere la porta chiusa e comunicare attraverso uno spioncino o una finestra.
2. Non fidarti subito: anche se sembrano persone distinte e per bene, ricorda che spesso l'apparenza inganna.
3. Controlla l'identità: se qualcuno si presenta come funzionario delle forze dell'ordine, chiedigli di identificarsi. Le forze dell'ordine, di norma, non operano mai da sole e sono sempre in uniforme, quasi mai in abiti civili.
4. Verifica prima che ci sia un'auto di servizio parcheggiata nei dintorni.
5. Non esitare e non aver paura di chiedere il motivo della visita. I veri funzionari sono abituati a fornire spiegazioni chiare e dettagliate.

È fondamentale ricordare che, in caso di dubbi, è sempre consigliabile contattare le autorità competenti per verificare l'identità di chi bussa alla porta.
Non esitare a chiedere informazioni e, se necessario, a richiedere l'intervento di agenti veri. **CHIAMA IL 112.**
Gli anziani e le persone fragili dovrebbero essere educati a riconoscere queste frodi.

Le famiglie devono svolgere un ruolo attivo nell'informare i propri cari su questo tipo di rischi e sulle strategie preventive.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

a. I FALSI AMICI

Possono presentarsi a casa vostra come amici di un parente o di un conoscente.

Immaginate di essere a casa, immersi nel profumo del caffè appena fatto. È un momento di tranquillità, un attimo di relax che vi siete concessi dopo una lunga giornata. Ma quel momento di pace può facilmente trasformarsi in qualcos'altro se, all'improvviso, sentite bussare alla porta. In un'epoca in cui la sicurezza sembra essere sempre più precaria, è fondamentale prestare attenzione a chi ci troviamo di fronte quando si tratta di aprire la nostra porta. Immaginiamo che si presentino alla porta "amici" di parenti o di conoscenti. "Ciao, sono un amico di Marco!" potrebbero dire. Oppure: "Salve, sono venuto per conto di Francesca." Queste frasi, spesso pronunciate con un sorriso rassicurante, possono sembrare innocue, ma rappresentano potenziali rischi.

Questi "falsi amici" sanno esattamente come tessere una rete di fiducia in pochi secondi per accedere ai vostri spazi privati e possono utilizzare i nomi di persone fidate per abbattere le barriere della diffidenza. In questi casi, è essenziale rimanere vigili e riflessivi.

La prima regola da seguire è dunque quella di non aprire la porta.

Ci sono numerosi motivi per cui questa decisione è fondamentale:

1. Sicurezza domestica: la vostra casa è il vostro rifugio e in nessun modo dovete comprometterne la sicurezza. Le statistiche sui furti e sulle truffe dimostrano che molte di queste situazioni iniziano proprio con un apparente "colpo di scena" radicato nella semplicità di un saluto amichevole.

2. Identificazione: Prima di far entrare qualcuno nella vostra casa, è giusto fare delle verifiche. Chiediamo prima di tutto: “Chi sei? Cosa vuoi?”. Si può anche fare una semplice telefonata al parente o l’amico in questione per accertarsi dell’identità.

3. La Trappola dell’Empatia: Le persone tendono a fidarsi degli estranei se questi appaiono vulnerabili. “Ho bisogno di aiuto” o “Ti prego, dammi solo qualche euro” sono frasi che possono mettere a dura prova il nostro cuore. Ma l’empatia, se non accompagnata da una valutazione critica della situazione, può portarci a prendere decisioni avventate.

Se vi trovate in una situazione simile, dovete essere preparati. Ecco alcuni suggerimenti su come affrontare la situazione senza aprire la porta:

- Se qualcuno bussa alla vostra porta, non abbiate paura di rispondere dall'interno. Fate domande e ascoltate attentamente le risposte. Ricordate: voi avete il diritto di proteggere la vostra privacy e la vostra sicurezza.

- Utilizzare i dispositivi di sicurezza: Oggi, molti di noi hanno videocamere o campanelli smart. Questi strumenti non solo vi permettono di vedere chi è alla porta, ma possono anche fungere da deterrenti per potenziali truffatori.

- Non cedere alla pressione: Se vi sentite attratti dalla narrazione di qualcun altro, ricordatevi di mantenere la calma. Anche se le parole sembrano persuasive, la vostra sicurezza vale molto di più. Se, purtroppo, vi trovate nella situazione in cui il truffatore è entrato in contatto con voi, mantenete la lucidità. Non fornire mai denaro o informazioni personali. Annotate eventuali dettagli riconoscibili e **CONTATTATE IL 112.**

Condividere storie e avvertimenti su tentativi di truffa può costruire una rete di protezione collettiva. Se sapete che ci sono stati altri casi nella vostra zona o che qualcuno sta cercando di frodare i vostri conoscenti, avvisare gli altri è un atto di responsabilità civica.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

b. IL FINTO CORRIERE

Non di rado capita che un corriere si presenti alla vostra porta chiedendo il pagamento di una somma di denaro per la consegna di un pacco. Questi individui sostengono che la merce sia stata ordinata dai vostri figli, parenti o altre persone del vostro condominio.

1. Se ricevete un avviso di consegna, accertatevi che i destinatari siano effettivamente a conoscenza dell'ordine. Contattateli prima di procedere.
2. Non ritirate pacchi inaspettati: se non vi è stata data alcuna informazione preliminare riguardo a questo pacco, non ritiratelo.
3. Non effettuate pagamenti prima di avere conferma. Se il corriere vi sembra insistente **CHIAMATE IL**

NUMERO UNICO EUROPEO PER LE EMERGENZE



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

c. IL FINTO AGENTE ASSICURATIVO

Negli ultimi anni l'aumento dei prezzi delle assicurazioni ha reso molti consumatori vulnerabili a offerte ingannevoli. Non è raro, quindi, imbattersi in un sedicente agente assicurativo che bussa alla vostra porta o si presenta nei pressi di un bancomat all'interno di un centro commerciale. Con un sorriso accattivante e frasi persuasive, questi individui si propongono di offrirvi polizze assicurative per la vostra famiglia, auto o casa a prezzi estremamente competitivi.

La tentazione di risparmiare è forte e, in un momento di crisi economica, molti possono cadere nella trappola. Dopo una lunga conversazione e qualche promessa allettante, si arriva al momento cruciale: il pagamento. Con una certa fretta, l'agente vi fa firmare documenti che sembrano ufficiali e vi consegna un foglio di carta, apparentemente una polizza assicurativa. Tuttavia potrete scoprire con grande sorpresa che quel documento non ha alcun valore legale.

La disillusione si trasforma rapidamente in preoccupazione: avete appena speso soldi per qualcosa di completamente inutile. È fondamentale, quindi, prestare attenzione e diffidare di offerte troppo belle per essere vere. Prima di sottoscrivere qualsiasi polizza, è consigliabile fare ricerche, controllare le credenziali dell'agente e confrontare le offerte autentiche sul mercato. La prudenza è la chiave per proteggere non solo il proprio portafoglio, ma anche la propria tranquillità. **CHIAMATE il 112.**



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

d. IL FINTO AVVOCATO O APPARTENENTE ALLE FORZE DELL'ORDINE

È certamente una situazione angosciante: ricevere una telefonata da un avvocato, carabiniere, finanziere o poliziotto, o dal centralino di un ospedale che ti informa che tuo figlio o nipote ha avuto un grave incidente e si trova in ospedale, oppure è stato arrestato e ha urgente bisogno di aiuto economico. Queste notizie sono devastanti e possono suscitare immediatamente paura e ansia. Tuttavia, è fondamentale mantenere la calma e saper riconoscere se si tratta di una truffa.

I truffatori si approfittano delle emozioni forti, creando scenari urgenti e drammatici per costringerti a reagire impulsivamente. Spesso, ti chiedono di inviare denaro immediatamente o di accompagnarli al bancomat per prelevare somme ingenti.

Non agire d'istinto: prendi tempo per riflettere e analizzare la situazione.

Tuttavia ci sono dei segnali di allerta ai quali bisogna prestare attenzione:

1. La richiesta urgente di denaro.

2. Nessuna conferma: se non ti viene fornito alcun dettaglio verificabile sul presunto incidente o problema legale, sii sospettoso.

3. Incertezze nei dettagli: potrebbero essere vaghi sui fatti, sul luogo dell'incidente o sulla natura del fermo. Chiamate sempre il

NUMERO UNICO EUROPEO PER LE EMERGENZE





Cosa fare se ricevi una chiamata del genere?

- Non rispondere impulsivamente: prenditi un momento per pensare e verifica la veridicità della chiamata.
- Contatta direttamente il tuo familiare: chiama tuo figlio o nipote per confermare la situazione. Se non riesci a contattarli, parla con altri familiari o amici.
- Non lasciare entrare nessuno: se un presunto "complice" dei truffatori si presenta a casa tua, non aprire la porta. Non farti convincere a consegnare denaro o a seguirli in nessun caso.
- Incoraggia anche altri membri della famiglia e amici a riconoscere questi segnali di allerta e a mantenere un atteggiamento scettico verso richieste di denaro urgenti. Essere informati è il primo passo per proteggersi e tutelarsi contro queste frodi.

  Rimanere vigili e precisi è essenziale. Ricorda: nel dubbio, verifica sempre!

  Se sospetti di essere vittima di una truffa **chiamate il 112**. Ogni informazione utile può aiutare a bloccare i truffatori.

© Cavoli Sergio 2025 – "Vademecum contro le Truffe: Insieme siamo più forti"

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l'autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

e. COME PROTEGGERE LA CASA

Vivere in un’abitazione sicura è il sogno di tutti e con alcuni semplici accorgimenti la nostra casa può esserlo. I ladri prediligono le abitazioni isolate, silenziose, senza barriere.

Può essere utile:

- la reciproca collaborazione tra vicini di casa, per restare in contatto se necessario e in tal modo ci sarà comunque qualcuno che controllerà la vostra abitazione durante la vostra assenza, breve o lunga che sia;
- chiudere sempre il portone d'accesso al palazzo;
- nascondere le chiavi di casa in posti sicuri e ben nascosti;
- non aprire il portone o la porta di casa se non si è certi dell’identità di chi ha bussato;
- installare una porta blindata con spioncino digitale;
- non lasciare i documenti personali in luoghi facilmente accessibili;
- installare dei dispositivi antifurto, e/o di videosorveglianza. Attivate sempre l'allarme ogni volta che uscite di casa e, se possibile, anche quando andate a dormire. Oggi ci sono agevolazioni fiscali per questo tipo di interventi.
- Non attaccate al portachiavi delle targhette con nome e indirizzo che possano, in caso di smarrimento, far individuare facilmente
  l’ appartamento;
- illuminate con particolare attenzione l'ingresso e le zone buie;
- mettete delle **grate alle finestre o dei vetri antisfondamento** se abitate in un piano basso, o in una casa indipendente. Oggi ci sono agevolazioni fiscali per questi interventi.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



- **Se vivete in una casa isolata o, se ne avete la possibilità,**

valutate l'adozione di un cane**.**

Un cane non è solo un fedele compagno e fonte di affetto, ma diventa anche un prezioso alleato nella sicurezza domestica: la sua presenza e il suo abbaiare possono scoraggiare intrusioni, mentre prendersene cura aumenta la vigilanza, la consapevolezza dell'ambiente circostante e la sensazione di protezione, indipendentemente dal piano in cui abitate.



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

- Quando andate **in vacanza non postate foto o informazioni** sui social network. Potrete farlo solo al vostro rientro. Informate della vostra assenza solo i vostri cari. Se il vostro viaggio o lavoro vi terrà lontano da casa per molto tempo è sempre meglio incaricare un familiare o un amico fidato di effettuare controlli saltuari.

- Se vi spostate per un weekend, o se siete soli in casa, in assenza di sistemi di sicurezza, lasciate accesa una luce o la radio in modo da mostrare e far sentire all'esterno che la casa è abitata. I ladri oggi cercano principalmente soldi, può essere utile lasciare anche qualche banconota di grosso taglio con un biglietto con scritto: “non ci sono altri soldi in casa e neanche gioielli, per favore non fate danni”.

- Una volta dentro, i **“**topi di appartamento” cercano di andare prima in camera da letto per poi passare ai luoghi meno scontati. Dagli armadi ai vestiti, alla cassetta del wc, dai cuscini del divano al barattolo dello zucchero, al vaso, al quadro, ogni cavità verrà esplorata.

- Al vostro rientro a casa, se vi accorgete che la serratura è stata manomessa o che la porta è socchiusa, o la persiana divelta, non entrate in casa, **chiamate il 112.**

- Ugualmente, se vi accorgete, appena entrati a casa, di essere stati derubati, non toccate nulla e telefonate subito al **112**.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

IV. PER STRADA

a. NEL PARCHEGGIO DEL SUPERMERCATO

All'uscita dei supermercati, spesso ci si imbatte in persone disponibili ad offrirci un aiuto per spingere il carrello o per portare la busta della spesa fino alla macchina o a casa. Questo gesto di gentilezza sembra innocuo e anche cortese, ma dietro a questo servizio può nascondersi una realtà ben più inquietante.

È fondamentale essere cauti e consapevoli del fatto che, in alcuni casi, queste figure possono avere intenzioni malevole. Il loro obiettivo non è solo quello di alleviare il peso delle nostre buste, ma anche di raccogliere quante più informazioni possibili su di noi.

Potrebbero essere disponibili ad accompagnarci alla posta, in banca o persino verso il bancomat, per captare dettagli cruciali riguardanti le nostre abitudini quotidiane, i luoghi che frequentiamo e, in alcuni casi, informazioni personali sui nostri conti e risparmi. Un sorriso e un gesto benevolo possono mascherare intenti meno nobili.

È importante, quindi, rimanere sempre vigili e proteggere i propri dati personali perché le informazioni raccolte potrebbero essere utili per derubarti anche successivamente!

112 NUMERO UNICO EUROPEO PER LE EMERGENZE.





© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

b. VICINO ALLA BANCA O ALLA POSTA

Se una persona si avvicina a voi, in particolare dopo che avete prelevato contanti da una banca o da un ufficio postale, fate attenzione! Spesso, questi individui possono presentarsi come impiegati della Banca o della Posta, sostenendo, per esempio, di dover controllare i numeri di serie delle vostre banconote perché potrebbero essere contraffatte.

Ricordate: nessun dipendente della Banca o dell'Ufficio Postale vi fermerà o verrà mai a casa vostra per controllare le banconote appena ricevute! Questa è una truffa ben nota. L'obiettivo del malvivente è semplice: ottenere il vostro denaro legittimo, sostituendolo con banconote false o sequestrandolo completamente.

Non consegnate mai i vostri soldi: se qualcuno vi fa questa richiesta, mantenete la calma e non cedete. Se sei ancora in strada attira l'attenzione dei passanti e **CHIAMA IL 112.**

© Cavoli Sergio 2025 – "Vademecum contro le Truffe: Insieme siamo più forti"

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l'autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

c. IN UN PARCO o PER LA STRADA

- **Una spinta di troppo.**

Immagina di trovarti a sorseggiare un caffè o una bibita fresca, osservando, per esempio, un gruppo di bambini che gioca. Ti si avvicina casualmente una persona con un passeggino, o una donna intenta a fare jogging, che, con un gesto distratto, colpisce il tuo bicchiere, rovesciando il liquido su di te. “Mi scuso tanto!” esclama, mentre si affretta a offrire aiuto, con uno sguardo premuroso.

Ma ecco il trucco: mentre si china per pulire il disastro che ha creato, la sua mano si muove rapidamente verso il tuo zaino o la tua borsa.
In pochi secondi riesce a rubare il portafoglio, il cellulare o persino le chiavi di casa, e se ne va con la scusa di aver lasciato cadere qualcosa.
Non solo questo schema può essere orchestrato da donne con bambini, ma anche da uomini che approfittano della situazione.
Immagina un ragazzo che, con un sorriso affabile, si avvicina per chiedere informazioni. Magari si tratta di un trucco ben congegnato: mentre ti distrae con la conversazione, un suo complice si aggira nei pressi della tua borsa, pronto a cogliere l’attimo. La cosa allarmante è che queste tattiche di furto avvengono troppo velocemente, mentre le vittime, ignare e fiduciose, credono di trovarsi di fronte a persone benintenzionate. La condivisione di momenti familiari e l’ambiente amichevole possono rendere difficile percepire il pericolo imminente. Pertanto è fondamentale rimanere vigili anche nei luoghi più innocui. È importante proteggere i propri beni e la propria sicurezza senza lasciare spazio agli approfittatori.
Non è mai sbagliato essere cauti. Anche nei momenti di apparente normalità possono nascondersi insidie pronte a coglierti impreparato.
La consapevolezza è la migliore difesa contro questi malfattori. Se purtroppo sei stato vittima di uno di questi raggiri, **chiama subito il 112.**



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **La truffa dell’abbraccio**

L’inganno dell’illusione: giovani donne e la trappola dei raggiri.
Negli ultimi anni si è assistito a un fenomeno sempre più preoccupante che coinvolge giovani donne e uomini anziani. Queste interazioni, che all’apparenza sembrano innocue o addirittura lusinghiere, nascondono spesso intenti malevoli. Giovani donne, con il loro atteggiamento gentile e affascinante, si avvicinano a uomini più maturi creando l’illusione di una connessione emotiva o seduttiva. Questa dinamica può essere vista come una forma di inganno che sfrutta la vulnerabilità degli anziani.
L’interazione inizia con complimenti e un comportamento affettuoso. Le donne spesso utilizzano frasi dolci e gesti amichevoli, facendo sentire le loro vittime speciali e importanti. Questo approccio può illudere gli anziani, facendogli credere che ci sia un reale interesse romantico o sessuale. Quando l’anziano, magari speranzoso di intraprendere un gioco di seduzione, rifiuta le avances, la situazione prende una piega inaspettata. A questo punto, queste donne non si fanno scrupoli: continuano a dimostrare affetto, avvicinandosi per un abbraccio che potrebbe sembrare innocuo. Tuttavia, proprio in quel momento, avviene il vero colpo di scena: le mani abili e rapide si muovono furtivamente per portare via portafogli, cellulari o orologi. La vittima, presa alla sprovvista, si ritrova spiazzata, confusa e, spesso, impotente di fronte a un atto così subdolo. Questo tipo di frode non solo ha conseguenze materiali per l’anziano derubato, ma lascia anche segni profondi sul piano emotivo. La fiducia viene infranta e il senso di sicurezza svanisce, lasciando spazio a una diffidenza che può influenzare negativamente le interazioni future. È fondamentale, quindi, sensibilizzare su questo tema e incoraggiare le persone, soprattutto quelle più vulnerabili, a mantenere un approccio critico e cauto nei confronti delle nuove conoscenze. Se sei vittima di questo tipo di raggiro, non esitare: **CHIAMA IL 112.**



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

- **Il finto malessere**

Per le strade affollate della città, potresti incorrere in situazioni che, a prima vista, sembrano richiedere il tuo intervento. Talvolta una persona potrebbe simulare un malore accasciandosi al suolo con l'aria disperata di chi ha bisogno di aiuto. L'istinto ci spinge ad avvicinarci, a cercare di capire come possiamo assistere chi sembra in difficoltà. Tuttavia, è fondamentale rimanere vigili e consapevoli.

In questi frangenti, la realtà potrebbe essere ben diversa. Il malore potrebbe essere solo una finzione, un abile inganno orchestrato da malintenzionati. Mentre ti avvicini per prestare soccorso, un complice – che si mimetizza tra la folla – potrebbe colpire. In un attimo di distrazione ti ritrovi a chiedere aiuto, a guardare un'ambulanza che non arriva, mentre il ladro chino vicino a te afferra la tua borsa o il tuo portafoglio, svanendo nel caos circostante. Questa modalità di truffa, purtroppo, è più comune di quanto si pensi. Non è solo una questione di mancanza di empatia o bontà d'animo; è importante preservare non solo il nostro benessere, ma anche quello degli altri.
Cosa fare quindi in queste situazioni?

- Osservare attentamente. Se noti qualcuno che appare in difficoltà, valuta la situazione con calma.
- Non avvicinarti immediatamente; cerca di capire se ci sono altre persone attorno, se la persona riceve già assistenza da qualcun altro.
- Chiamate il **112**

Ricorda che il tuo gesto di altruismo è lodevole, ma la prudenza deve sempre guidare le tue azioni. Mai sottovalutare la possibilità di un inganno. Essere attenti e cauti può salvaguardarti da spiacevoli sorprese e garantire che il tuo aiuto arrivi realmente dove serve.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Maghi e santoni**

Ancora oggi, nonostante viviamo in una società moderna ed evoluta, è sorprendente quanto possa essere diffuso il fenomeno dei maghi e dei santoni. Queste figure, spesso dotate di carisma e abilità persuasiva, riescono a catturare l'attenzione di persone vulnerabili, facendo leva sulla loro disperazione. Chi si trova ad affrontare gravi problemi di salute o difficoltà lavorative può essere tentato di cercare soluzioni alternative, spesso illusorie.

Molti di questi "professori" dell'occulto offrono promesse miracolose: guarigioni rapide da malattie incurabili, risoluzione di problemi economici o addirittura la fortuna in amore. Tuttavia, dietro a tali affermazioni si nasconde una realtà ben più amara: la manipolazione delle emozioni umane per trarne profitto. Le persone, in particolare gli anziani, nella loro ricerca di aiuto, sono vittime di queste frodi, e arrivano a spendere somme considerevoli per riti e pratiche che non hanno alcun fondamento scientifico.

In Italia fare il mago è vietato. La legge punisce l'esercizio della pseudoscienza, riconoscendo il diritto dei cittadini a ricevere cure e supporto validi e basati su evidenze concrete. È fondamentale ricordare che, per ogni problema, è sempre consigliabile rivolgersi a professionisti qualificati: medici, psicologi e specialisti. Solo affidandosi a queste figure si possono ottenere diagnosi accurate e cure adeguate, evitando di cadere nelle trappole di chi sfrutta la fragilità altrui.

Non esitare, **CHIAMA il 112.**



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **L’inganno della borsa.**

Tra le bancarelle puoi essere attratto da una piccola esposizione di borse artigianali. Appena ti avvicini, il commesso ti invita a provarne una. Mentre il venditore finge di essere distratto, ti accorgi che all’interno c’è, per esempio, un portafoglio pieno di banconote. Senza indugio acquisti la borsa, cercando di non attirare l’attenzione del commesso. Appena ti allontani dalla bancarella, la curiosità di scoprire quel tesoro è troppo grande, ma scopri che quelle che sembravano banconote sono pezzi di carta straccia! Chiama subito il

NUMERO UNICO EUROPEO PER LE EMERGENZE.





© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **L’inganno del giubbotto.**

Lo sguardo ti cade su una bancarella che espone giubbotti. Incuriosito, ti avvicini e il venditore ti invita a provarne uno. Mentre indossi il giubbotto, senti un oggetto nella tasca e trovi, per esempio, un orologio scintillante. “Un Rolex! Incredibile!”, pensi. Compri il giubbotto senza pensarci due volte. C’è qualcosa di elettrizzante nell’idea di possedere un capo d’abbigliamento accompagnato da un orologio di valore. Pochi istanti dopo, mentre ti allontani con il nuovo giubbotto, apri la tasca.

Quell’affare che sembrava così vantaggioso si rivela un’illusione: l’orologio era un falso ben fatto, ma pur sempre un falso. E il giubbotto? Non valeva nemmeno la metà del prezzo pagato.

Entrambe le esperienze insegnano una lezione preziosa. La tentazione di un affare imperdibile può farci perdere la lucidità. È facile farsi prendere dall’emozione del momento, ma è fondamentale rimanere vigili e cauti.

Le bancarelle per strada possono offrire tesori inaspettati, ma anche inganni travestiti da opportunità. Il mondo è pieno di truffatori pronti a sfruttare l’ingenuità delle persone. **Chiama sempre il 112.**

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **L’inganno del finto fruttivendolo**

Nelle vicinanze dei mercati o nei parchi cittadini è facile imbattersi in una scena che suscita simpatia e compassione: un uomo, con un’espressione triste e gli occhi lucidi, si avvicina a te. La sua voce tremante racconta una storia straziante: ha perso il lavoro per rimanere accanto alla moglie malata o al figlio in gravi condizioni. Ti parla delle spese sanitarie insostenibili, del bisogno disperato di aiuto e di come ha deciso di vendere frutta o verdura per cercare di far fronte alle emergenze.

L'immagine di una famiglia in difficoltà tocca le corde più profonde della tua anima. Ti offre la merce, presentandola come fresca e di ottima qualità. Senza pensarci troppo, decidi di aiutarlo, pagando una cifra ben superiore al reale valore di quei prodotti. Lo vedi caricare la frutta o la verdura nel tuo bagagliaio, con un'espressione di gratitudine che sembra sincera.

Ma quando torni a casa ti accorgi che quella frutta e quella verdura, sebbene appaiano belle e fresche, in realtà sono prodotti di scarsa qualità. Si può **chiamare il 112** perché non è solo una questione di frode, ma un passo necessario per fermare chi sfrutta la buona fede delle persone.

112 NUMERO UNICO EUROPEO PER LE EMERGENZE





© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **La deviazione**

Ti trovi in una stazione affollata, il brusio della gente riempie l'aria, i treni arrivano e partono senza sosta, le voci si intrecciano, qualcuno si ferma, qualcuno corre, e tu hai solo una direzione in mente, un'uscita da raggiungere dentro quel flusso continuo.

A un certo punto una persona si avvicina con naturalezza, come se fosse normale parlarti lì in mezzo a tutta quella confusione, e ti dice che da una parte è tutto chiuso, che non ha senso andare avanti così e che è meglio passare dall'altro lato, più veloce, più semplice, e lo dice con una sicurezza tranquilla, senza esitazioni.

E senza che ci sia davvero un momento in cui te lo chiedi, ti ritrovi a seguirlo. All'inizio non cambia nulla, la stazione è ancora la stessa, i rumori familiari, i movimenti intorno, tutto sembra normale, ma mentre cammini qualcosa inizia lentamente a spostarsi, la folla si dirada senza che tu lo noti davvero, i suoni si attenuano, i passaggi diventano più stretti, e il percorso cambia senza un segnale preciso.

Poi arriva quella sensazione difficile da spiegare, come se i punti di riferimento che avevi prima non fossero più gli stessi, come se stessi andando avanti ma senza riconoscere del tutto la direzione, e continui comunque a camminare perché ormai sei dentro quel tragitto e tornare indietro non è più immediato come sembrava all'inizio.

E più vai avanti, più tutto si sposta, fino a quando il posto in cui ti trovi non assomiglia più davvero a quello da cui eri partito, anche se non c'è mai stato un istante preciso in cui puoi dire che qualcosa è cambiato.

Ed è proprio lì che tutto può ancora essere interrotto.

Fermati un attimo, senza fretta, come se stessi semplicemente riprendendo fiato, guarda intorno e riconosci ciò che ti circonda, e se qualcosa non ti convince o non ti sembra più chiaro, non continuare per inerzia: saluta con naturalezza, ringrazia e torna indietro verso un luogo che conosci.

Se ti senti incerto o a disagio, non restare da solo dentro quella sensazione. Avvicinati ad altre persone, resta in zone più frequentate, oppure chiedi aiuto a chi è vicino, perché la presenza degli altri cambia subito la percezione di quello che stai vivendo.

E se qualcosa non torna, anche solo per un attimo, è già il momento di fermarsi e, nel dubbio, chiamare il 112.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Il cerchio**

Sei in una fermata, in un parco o in fila da qualche parte, in uno di quei momenti in cui stai semplicemente aspettando e le persone attorno continuano a muoversi senza che tu ci faccia troppo caso.
A volte qualcuno si avvicina con un telefono o delle cuffie e ti dice “ti faccio ascoltare una cosa”, altre volte è una semplice domanda, un’informazione, qualcosa che sembra innocuo e normale, e in entrambi i casi ti fermi senza pensarci troppo, perché è una situazione che sembra parte della quotidianità.
Ed è proprio mentre sei lì, con l’attenzione su quella persona, che la scena cambia senza un passaggio evidente.
Arrivano altre persone, quattro o cinque, quasi senza rumore, e in pochi secondi si avvicinano troppo, creando uno spazio chiuso intorno a te mentre tutto avviene in modo rapido e coordinato, le mani si muovono veloci, borse aperte, tasche frugate, mentre la tua attenzione è ancora legata a quell’istante iniziale.
Quando provi a reagire e capisci che qualcosa non torna, il gruppo si è già sciolto, ognuno si allontana in una direzione diversa, mescolandosi tra la gente come se non fosse mai successo nulla.
Ed è proprio lì che tutto si gioca in pochi secondi.
Non restare fermo a cercare di capire subito cosa è successo: crea distanza, allontanati con decisione dal primo contatto e spostati verso uno spazio più aperto e frequentato.
Se qualcuno prova ancora a parlarti o a trattenerti, non fermarti a discutere: una risposta breve, mentre continui a muoverti, come “mi spiace, devo andare”, è più che sufficiente.
Cerca subito un punto sicuro, una persona riconoscibile, un negozio, un gruppo di persone, qualcosa che ti riporti dentro un contesto chiaro e controllabile, e solo dopo, con calma, verifica cosa è successo.
Condividi quanto accaduto con familiari e conoscenti, perché riconoscere questi schemi aiuta a evitarli.
E se qualcosa non torna, non aspettare: chiama il 112.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Due minuti**

Sei in una strada, in una stazione o in una piazza, immerso nel passaggio continuo delle persone, quando qualcuno ti passa accanto, lascia vicino a te uno zaino o un pacco e ti dice con naturalezza “me lo tieni un secondo”, come se fosse la cosa più normale del mondo, e senza darti il tempo di rispondere si allontana già tra la folla.

Rimani lì con quell’oggetto accanto, dentro una situazione che si è creata in pochi istanti mentre tutto continua a muoversi intorno a te.

Poco dopo arriva un’altra persona, lo sguardo cade prima sull’oggetto e poi su di te, e iniziano delle domande semplici ma insistenti: se sia tuo, cosa contenga, perché si trovi lì, come se in qualche modo tu fossi già dentro una situazione che sta prendendo forma.

E mentre provi a rispondere, l’attenzione si concentra tutta su quel punto, mentre il resto intorno continua a scorrere ma perde importanza, diventa sfondo.

Ed è proprio lì che tutto si gioca in pochi secondi.

La cosa importante è non restare coinvolto: fai subito un passo indietro, allontanati con calma, lascia l’oggetto dov’è e spostati verso uno spazio più aperto o verso altre persone, dove la situazione si spezza e torna tutto più chiaro.

Se qualcuno insiste o cerca di trattenerti, non fermarti a spiegare: una frase breve, senza rallentare il passo, come “non è mio, non ne so nulla”, e continui ad allontanarti.

E se hai anche solo un dubbio o ti senti in difficoltà, non esitare a chiamare il 112.

© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



V. IN BICICLETTA

Quando si decide di spostarsi in bicicletta, è fondamentale prestare attenzione non solo alla sicurezza personale, ma anche a quella dei propri beni. Un errore comune che molti ciclisti commettono è quello di riporre borse o marsupi nel cestello anteriore della bicicletta. Sebbene possa sembrare una soluzione comoda e pratica, ci sono diversi motivi per cui è consigliabile evitare questa abitudine.

In primo luogo, il cestello è un luogo facilmente accessibile sia per il ciclista che per eventuali malintenzionati. Lasciare oggetti di valore in vista aumenta notevolmente il rischio di furto. Anche se ci si allontana solo per un momento, un ladro esperto potrebbe approfittarne per sfilare rapidamente la borsa o il marsupio senza farsi notare.

In secondo luogo, il posizionamento di oggetti pesanti o ingombranti nel cestello può comprometterne l'equilibrio. Avere un carico sbilanciato può rendere la manovrabilità della bicicletta difficoltosa, aumentando il rischio di cadute o incidenti. La sicurezza durante la pedalata deve sempre essere la priorità.

Infine, un altro aspetto da considerare è la protezione dei propri beni. Un cestello aperto non offre alcuna protezione contro le intemperie. Se piove o se c'è vento, i tuoi effetti personali potrebbero danneggiarsi.

La soluzione ideale è, dunque, utilizzare una borsa da bici appositamente progettata, che può essere montata sul telaio o sulla schiena.

In sintesi, quando si viaggia in bicicletta, è meglio evitare di riporre borse o marsupi nel cestello. Opta per alternative più sicure e mantieni i tuoi beni protetti, così potrai goderti la tua passeggiata in tutta tranquillità.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

VI. SUI MEZZI PUBBLICI

Quando ci si sposta in autobus o in metropolitana, la sicurezza dei propri effetti personali diventa una priorità fondamentale. I mezzi pubblici, pur essendo un modo efficiente per muoversi in città, possono anche rappresentare un terreno fertile per i furti e le distrazioni.

Ecco perché è essenziale adottare alcune misure preventive:

- tenere il portafoglio nella tasca anteriore dei pantaloni perché questa collocazione riduce sensibilmente il rischio di furto e consente di avere sempre sotto controllo la situazione, evitando di dover scavare in borse o zaini ogni volta che si deve pagare un biglietto o mostrare un documento;
- portare la borsa davanti sul petto. Tenere la borsa a tracolla o in una posizione centrale non solo rende più difficile per un ladro avvicinarsi furtivamente, ma consente anche di avere una maggiore visibilità su ciò che accade attorno a noi. Nella folla è meglio essere consapevoli di eventuali movimenti sospetti e, al contempo, proteggere i propri beni in modo più efficace;
- scegliere borse con cerniere sicure e diverse tasche può aiutare a organizzare meglio gli oggetti personali, rendendo più difficile per i malintenzionati accedere a tutto in un colpo solo;
- usare materiali resistenti e colori meno appariscenti può anche contribuire a mantenere un profilo basso, evitando di attirare l'attenzione su oggetti di valore;
- mantenere sempre una certa vigilanza e prestare attenzione all'ambiente circostante. Essere coscienti del proprio spazio e delle persone intorno a noi può fare la differenza tra un viaggio tranquillo e un'esperienza stressante. Con un po' di attenzione e precauzione, è possibile godere dei vantaggi dei mezzi pubblici senza correre rischi.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

VII. IN MACCHINA

- **Alla guida**.

In macchina è fondamentale adottare alcune precauzioni per garantire la propria sicurezza e quella dei propri beni. Un aspetto spesso sottovalutato è il fatto di non lasciare mai borse o marsupi sul sedile del passeggero, soprattutto con il finestrino aperto. Questa situazione è un invito per i ladri, perché rende più facile un eventuale furto.

Al semaforo o in coda nel traffico la tua attenzione potrebbe essere focalizzata su altro e se qualcuno si avvicina alla tua automobile, con un gesto rapido e discreto, la tua borsa viene sottratta senza che tu te ne accorga. Questo scenario, purtroppo, è più comune di quanto si pensi.

Per evitare queste situazioni, abituiamoci a **tenere il finestrino alzato e sempre la portiera chiusa e bloccata con la sicura**, specialmente quando ci troviamo in aree affollate o poco raccomandabili. Non solo proteggeremo i nostri effetti personali, ma ci sentiremo anche più al sicuro all'interno del veicolo.

Questa abitudine può fare un'enorme differenza nella prevenzione dei furti in auto.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

NUMERO UNICO EUROPEO PER LE EMERGENZE



Se urtate, durante la guida, un altro veicolo o un pedone e il conducente scende mostrando un danno sulla carrozzeria della sua auto, o il pedone lamenta di essere stato urtato alla gamba, potrebbe chiederti di essere risarcito in via amichevole con una piccola somma di denaro in contanti. In questi casi la cosa più saggia da fare è rimanere all'interno della propria auto e **chiamare immediatamente il 112** per segnalare l'accaduto, fornendo dettagli utili sul luogo e sull'identità delle persone coinvolte. Per proteggerti in situazioni come questa, potresti considerare l'acquisto di una dash cam (telecamera da cruscotto).

Oggi sono disponibili a prezzi accessibili e possono registrare tutto ciò che accade mentre siete alla guida.

Queste telecamere possono fornire prove preziose in caso di incidenti o tentativi di frode, garantendoti tranquillità e sicurezza sulle strade.

- **In sosta**.

Siete seduti in macchina in attesa di qualcuno: chiudete sempre le portiere con la sicura, e se qualcuno si avvicina per un'informazione, non abbassate mai il finestrino e aspettate che questa persona si allontani. Potrebbe essere un potenziale malfattore. La sicurezza personale deve sempre venire prima di ogni interazione casuale: nel mondo attuale, la prudenza deve diventare parte integrante delle nostre vite quotidiane.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

L’inganno della bottiglietta di plastica incastrata nelle auto.

I ladri, puntando su un veicolo specifico, posizionano una bottiglietta di plastica vuota nella gomma anteriore dell’auto. Questa manovra è particolarmente subdola, poiché il conducente raramente si accorge della presenza del corpo estraneo incastrato nella ruota. Quando il conducente accende il motore, il rumore prodotto dalla bottiglietta schiacciata attira la sua attenzione. L’automobilista, preoccupato, scende dall’auto per verificare cosa stia succedendo. È proprio in questo momento che i ladri entrano in azione: approfittando della situazione, spesso con il motore acceso e le chiavi inserite, portano via il veicolo in pochi secondi, lasciando il legittimo proprietario incredulo e impotente. Il successo di questa truffa si allinea ad altre tecniche fraudolente, come la truffa dell’adesivo o quella della ruota bucata, tutte caratteristiche di un'epoca in cui la disattenzione può costare cara. È cruciale, anche quando andiamo di fretta, prestare particolare attenzione alla propria vettura prima di mettersi alla guida, focalizzandosi sulle gomme e controllando eventuali particolari sospetti. Un piccolo dettaglio, anche se non apparente, potrebbe essere un segnale di pericolo. Anche **un carrello della spesa vuoto dietro la nostra auto** ci deve allarmare, così come **una banconota, in genere da 10 o 20 €, appoggiata sul parabrezza.** In ogni caso, unico accorgimento da seguire è di non uscire dall’auto, ma di allontanarsi rapidamente. Se ciò non fosse possibile, è importante assicurarsi che tutte le portiere siano ben chiuse e **chiamare subito il 112**, suonare il clacson per attirare l’attenzione di passanti o altri automobilisti.

Ricordare questi semplici passi può fare una grande differenza. La prevenzione è essenziale per contrastare questo tipo di criminalità. In un contesto in cui i furti d’auto sono in crescita, l'informazione e la consapevolezza possono essere gli alleati principali per evitare di diventare vittime di truffe ingegnose come quelle sopra esposte.



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

VIII. NEI LOCALI PUBBLICI

Quando si va a mangiare in un locale, è fondamentale prestare attenzione non solo al cibo, ma anche alla sicurezza dei propri effetti personali. Ecco alcuni consigli pratici per evitare furti o smarrimenti che possono rovinare la serata:

1. non lasciare **la borsa** incustodita. È un'abitudine comune appoggiare la borsa sul bracciolo della sedia, pensando che sia al sicuro. Tuttavia questa prassi può esporre i tuoi beni a furti. È preferibile tenere la borsa sempre in modo sicuro, magari posizionandola tra le gambe o utilizzando un gancio specifico per borse, se disponibile nel tavolo e comunque acquistabile con 5 €;
2. attenzione alla **giacca**: un altro errore frequente che facciamo è lasciare la giacca sulla spalliera della sedia, con anche oggetti di valore come il portafoglio. Niente di più facile per un malintenzionato che afferrare la giacca e fuggire o frugarvi all'interno. Se hai bisogno di toglierti la giacca, considera di appenderla a un attaccapanni o di tenerla sulle gambe;
3. attenzione allo **smartphone**: mai sul tavolo. Lo smartphone è uno degli oggetti più ambiti dai ladri. Oggi rappresenta la chiave di accesso alla nostra vita, non tutti sono in grado di bloccarlo e renderlo inutilizzabile. Appoggiarlo sul tavolo può sembrare comodo, ma offre un'opportunità perfetta per chiunque desideri rubarlo. È meglio tenerlo nella tasca della giacca o dei pantaloni.

   Mantieni sempre sott'occhio i tuoi effetti personali e goditi la serata in tutta tranquillità!



IX. TRUFFE INFORMATICHE

Oggi, con internet, il criminale non ha più un volto e…… non dorme mai. Basta un click fatto senza accorgersene perché riesca a entrare nelle nostre case e nelle nostre vite.

I pericoli online possono presentarsi in tanti modi e con diversi livelli di rischio.

Non avere paura né vergogna**.**

Se hai un dubbio o ti senti in difficoltà, chiedi aiuto e **chiama** il **112**."

112 NUMERO UNICO EUROPEO PER LE EMERGENZE



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***Man In The Middle***

Un primo esempio di questa attività illecita si chiama *man in the middle* (uomo in mezzo), il cui obbiettivo principale è quello di rubare le nostre informazioni. È una forma di attacco diretta ai router o server in cui una terza persona, il malfattore, intercetta e altera la comunicazione tra due parti, che credono di comunicare tra loro. Per esempio si pone tra vittima e server (come il caso, ad esempio, di un server di una banca online o di posta elettronica). Sono attacchi efficaci e difficili da individuare.

Come prima difesa, evitare di utilizzare reti wifi gratuite soprattutto se pensi di effettuare transazioni sensibili. Sarebbe meglio utilizzare un plug-in per browser in grado di stabilire connessioni sicure.

Non visitare i siti web quando il browser ci allerta di un problema nel loro certificato di sicurezza.

Se la pagina web che stai visitando ha iniziato a scaricare file automaticamente, senza il tuo permesso, quasi sicuramente questo sito è compromesso.

Aggiorna sempre l'antivirus, preferisci quelli che hanno un sistema interno di controllo delle pagine web che informa l'utente quando sta per entrare in un sito pericoloso.

Infine sarebbe preferibile avere un apposito computer solo per le transazioni.



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme siamo più forti”

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

- **Truffe col *Trading Online*.**

Anche in questo mondo le truffe non mancano, diffidare sempre da chi propone facili guadagni. Investire in borsa può essere allettante e vorremmo far fruttare i nostri risparmi con il *Trading online*.

Il ***TOL (trading online***) può essere fatto comodamente da casa e dal proprio computer e consiste nell'acquistare e vendere titoli finanziari da remoto. È un'attività rischiosa perché si guadagna sulla differenza di prezzo tra acquisto e vendita di azioni e obbligazioni. Non si può operare direttamente sui mercati finanziari. È necessario rivolgersi ad un broker finanziario, ossia un intermediario che acquista e vende titoli per conto del cliente. Il truffatore contatta l'ignara vittima, il più delle volte tramite un finto call center con il pretesto di offrire soluzione d'investimento facili e con grandi profitti. Sebbene titubanti, potremmo farci tentare e affidare piccole somme di denaro che ci si vedrà restituire velocemente con i primi guadagni. In quel momento i criminali chiederanno una somma maggiore con la falsa promessa del ritorno assicurato, e, ricevuto l'importo richiesto, il falso operatore di trading si dilegua, così la vittima non potrà recuperare quanto apparentemente investito.

Per fare trading ed evitare le truffe, la CONSOB ha messo a disposizione degli utenti una piattaforma di broker autorizzati all'esercizio della professione.

Se hai dubbi, **contatta la CONSOB al numero 06.8477611** (dal lunedì al venerdì, dalle 9.00 alle 13.00 e dalle 14.30 alle 16.30) e denuncia.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***Cryptolocker:***

È un virus “trojan” comparso per la prima volta nel 2013, perfezionato nel 2017. Questo malware è una forma di “**RANSOWARE”** che infetta i sistemi Windows e consiste nel criptare i dati della vittima, richiedendo un pagamento, un riscatto per la decriptazione. Ad oggi circa il 3% di chi è colpito da questo malware decide di pagare. Alcune vittime riferiscono che, pur avendo pagato il riscatto, non hanno visto i propri file decriptati. Non pagate, bensì segnalate!

- ***Digital Extortion:***

Con questo termine ci si riferisce all’attività posta in essere da criminali informatici con lo scopo di estorcere denaro ad un privato o un’azienda in cambio di non diffusione di dati provenienti da mail, siti pornografici visitati o altro materiale compromettente (sottratto tramite un **ramsonware)** che potrebbero ledere l’immagine di un soggetto e le sue relazioni sociali. Chiunque può cadere vittima di un attacco di estorsione digitale, da privati cittadini a celebrità a politici e aziende. Non aprite mail dubbie né scaricate file sconosciuti.

112 NUMERO UNICO EUROPEO PER LE EMERGENZE





© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Truffa Romantica:**

Il truffatore sceglie attentamente le vittime sui vari social (FaceBook, Instagram, Telegram, etc), crea profili falsi su siti e app di incontri, crea una storia verosimile e pubblica molto affinché il proprio profilo possa sembrare reale (le immagini e le foto del falso profilo sono prese da internet). Il truffatore non cerca sesso, le conversazioni sono sempre amichevoli, instaura una relazione con te per creare fiducia e dipendenza emotiva, così sarà più facile chiedere soldi per improvvise difficoltà economiche o per acquistare il biglietto per raggiungerti. Questo stratagemma funziona perché fa leva sul bisogno di sentirsi amati e valorizzati. Purtroppo questo tipo di truffa negli ultimi anni è in continua crescita, ma bisogna segnalare e avvisare il sito di social network o l'app in cui hai incontrato il truffatore.

112 NUMERO UNICO EUROPEO PER LE EMERGENZE





© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***Sex Extortion*:**

La sextortion è un reato grave che si verifica quando qualcuno minaccia di distribuire materiale privato e sensibile se non gli vengono fornite immagini di natura sessuale, favori sessuali o denaro.

I malintenzionati online potrebbero guadagnarsi la tua fiducia fingendosi qualcuno che non sono. Si nascondono anche nelle chat room e registrano chi pubblica o trasmette in streaming immagini e video sessualmente espliciti di sé stessi, oppure possono hackerare i tuoi dispositivi elettronici tramite malware per accedere ai tuoi file e controllare la tua webcam e il tuo microfono senza che tu te ne accorga.

- Non inviare mai immagini compromettenti di te stesso a nessuno, non importa chi sia o chi dica di essere.
- Non aprire allegati da persone che non conosci.
- Spegni i tuoi dispositivi elettronici e le webcam quando non li usi.
- Se sei ricattato, non pagare; interrompi ogni contatto e segnala subito.

Aiutateci a trovare questi criminali e a impedire loro di rovinare le vite delle persone.

112 NUMERO UNICO EUROPEO PER LE EMERGENZE





© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***The Evolution Of Triple Extortion***

È l'ultima evoluzione della precedente: i criminali crittografano i dati e li esfiltrano minacciando di farli trapelare se le richieste di riscatto non vengono soddisfatte. Se una vittima si rifiuta di pagare, i dati rubati possono essere messi all'asta sui forum del crimine informatico. Questo offre ai criminali un'altra strada per monetizzare le loro azioni illegali. Ma si sono spinti ancora oltre con schemi di tripla estorsione. In alcuni casi, crittografano e rubano dati, minacciano i dipendenti di un'azienda, contattano familiari e responsabili aziendali, e sovraccaricano i siti Web di traffico (noto anche come attacchi DDoS o Distributed Denial-of-Service) per costringere al pagamento. Talvolta nel messaggio ricevuto di minaccia è nascosto un **Trojan**.

© Cavoli Sergio 2025 – "Vademecum contro le Truffe: Insieme siamo più forti"

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l'autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Consigli per la compravendita di oggetti su siti Internet:**

Per le forze di Polizia è impossibile monitorare tutti i siti internet che fanno commercio elettronico in aggiunta alla massiccia diffusione di applicazioni di compravendita che propongono prodotti a prezzi vantaggiosi. Ecco perché i truffatori trovano terreno fertile e possono facilmente approfittarne per ingannare gli acquirenti offrendo prodotti inesistenti o contraffatti.

In aggiunta a questo fenomeno, vittima della truffa è la persona che mette in vendita il proprio bene. Viene contattata dal truffatore che, fingendosi un potenziale acquirente, è quasi sempre residente in altre città o al di fuori dei confini Italiani: questi individui vogliono in realtà appropriarsi dei dati personali per poi perpetrare altre truffe.

- Diffida da chi offre un prodotto ad un prezzo troppo economico.
- Diffida se l'acquirente si trova all'estero.
- Verifica la presenza del lucchetto per le transazioni sicure in alto a destra del sito e utilizza sempre un metodo di pagamento sicuro,(NO Western Union, carta regalo, ricariche…).
- Non inserire informazioni personali per riscattare un voucher o per sbloccare un fantomatico sconto.
- Non scaricare nessun software per completare l'acquisto.
- Non anticipare mai denaro per sospette operazioni doganali, spese e commissioni.
- Verifica la presenza dei dati dell'azienda (partita IVA, sede legale).

Diffidate sempre se il costo del bene che si vuole acquistare è nettamente inferiore a quello proposto sui siti ufficiali.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **La finta eredità:**

Chi non ha mai desiderato avere un ricco parente sconosciuto che ci lascia una ricca eredità? Attenzione, potreste essere contattati da un avvocato o notaio perché siete destinatario di una cospicua eredità, ma per entrarne in possesso dovrete consegnare un determinato importo ad una persona incaricata dal notaio.

Il programma *Striscia la notizia* ha documentato diversi casi simili in giro per l'Europa.

Non anticipare mai denaro quando sei tu che devi riceverlo. Ogni richiesta simile non è assolutamente legittima, perciò segnala sempre l'accaduto.

- **Pagamento PAYPAL:**

Utilizzi PayPal per i tuoi acquisti? Bene, però se effettui il pagamento con una dicitura non pertinente all'operazione, del tipo **"invia pagamento/invia regalo ad amici e familiari",** e il tuo acquisto non va a buon fine, sappi che **non potrai fare nessun reclamo.**

PayPal non protegge gli acquisti a meno che non si tratti di transazioni per beni o servizi**.**

- **Vincite a premi / lotterie**

Sempre più frequenti sono i messaggi SMS / WhatsApp con cui ti viene chiesto di pagare una piccola commissione di gestione pratica in cambio di splendidi premi, viaggi o soggiorni in Resort: questi sono di solito una truffa. Dopo aver pagato quanto richiesto tramite bonifico, carta regalo o criptovaluta, (sistemi di pagamenti sicuri per i malfattori) non ricevi nulla.

Non inviare denaro a nessuno che non conosci. La ricezione di un premio è gratuita, mi spiace disilluderti ma ti sei imbattuto in un truffatore.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***Phishing:***

È un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Il termine *phishing* è una variante di *fishing* (letteralmente "pescare" in lingua inglese) e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente.

Generalmente si riceve, sulla propria casella di posta elettronica (E-Mail) o tramite sms fittizi, l'avviso di un'anomala attività riscontrata sul conto corrente. Queste mail ed sms sono caratterizzati dalla presenza di un link che rimanda a un sito clone di quello della banca. Se inseriti i dati richiesti il truffatore ha piena disponibilità del conto corrente del malcapitato.

Bisogna sempre prestare attenzione ai seguenti segnali che possono aiutarti a individuare le truffe di *phishing*:

- nessuna banca invierebbe mai link di accesso diretto al proprio conto corrente online o a una pagina dove inserire i propri dati personali e bancari. Meglio diffidare di questi comunicati e, nel dubbio, accertarsene con il centro assistenza del vostro istituto di credito;
- molti messaggi di phishing sono scritti male e possono contenere errori di ortografia, di battitura e di grammatica;
- le email e i messaggi truffaldini ti indirizzeranno molto probabilmente a un sito Web non sicuro, perciò controlla sempre l'URL e l'ortografia del nome della società;
- non aprire email che contengono allegati, perché possono contenere virus che infetteranno il tuo dispositivo.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***Vishing*:**

È una truffa simile al *phishing*, fa leva sulla maggiore fiducia che le persone hanno nel contatto umano, ma lo scopo è identico, ovvero carpire con l'inganno informazioni private, **utilizzando il telefono**. L'operatore chiede alla vittima di fornire i propri dati, come il nome utente e il pin. Si suggerisce d'interrompere immediatamente la telefonata.

- ***Smishing:***

Lo *smishing* si differenzia dal *phishing* perché vengono utilizzati messaggi di testo all'interno di SMS convincenti che inducono i destinatari - grazie a un link presente nel messaggio - ad inviare le informazioni private richieste, o a scaricare programmi dannosi sul pc o smartphone.

- ***Pharming*:**

Un attacco informatico il cui **obiettivo è il furto di dati personali**. Il truffatore indirizza la vittima verso un sito web "clone" con un nome di dominio ufficiale attrezzato per carpire i dati personali della vittima o installare *malware* sul computer dell'utente, al fine di ottenere informazioni personali e finanziarie.

È un attacco molto difficile da rilevare, poiché i criminali informatici attaccano il DNS (Domain Name Server) con cui riescono a reindirizzare gli utenti su un sito web falso.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

NUMERO UNICO EUROPEO PER LE EMERGENZE



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- ***Trojan*:**

Con il termine "t*rojan*" ci si riferisce ai malware ad accesso remoto, che vengono installati nella macchina della vittima. Il malware raggruppa decine di sottocategorie (***Trojan-Proxy, Keylogger Trojans, Trojan-Spy*** etc**)** con un unico denominatore: carpire i dati sensibili rinchiusi all'interno dei propri computer.

I *trojan* non si diffondono autonomamente, spesso è la vittima stessa che involontariamente, non prestando attenzione alle mail ricevute oppure ai siti che sta visitando, scarica un trojan sul proprio computer. Recentemente sono stati identificati virus Trojan all'interno di file con estensione PDF.

© Cavoli Sergio 2025 – "Vademecum contro le Truffe: Insieme siamo più forti"

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l'autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Raccolta Fondi (*Fake Crowdfunding*):**

Il *crowdfunding* non è altro che una raccolta di fondi avviata generalmente per far fronte ad emergenze medico sanitarie anche a seguito di un terremoto, un'alluvione o per finanziare persone, Fondazioni o Associazioni per realizzare dei progetti meritevoli.

La truffa è composta da tre soggetti: il donatore, il ricevente ed il malfattore. Quest'ultimo ritrasmette o altera le comunicazioni tra le due parti; nello specifico dirotta i fondi verso un proprio conto corrente aperto presso banche estere. Spesso questa truffa è preceduta da attacchi *trojan* o *phishing*.

Questi attacchi informatici, sia che provengano da una mail sia da una telefonata o SMS, si sostituiscono ad una comunicazione ufficiale di un ente statale o un'azienda importante e hanno un obiettivo in comune, ingannare il destinatario per **estorcere dati sensibili**, accedere al conto corrente e alle carte di credito.

Ecco qualche consiglio per evitarlo:
1. Non fidarti mai di richieste sospette: Se qualcuno ti chiede informazioni personali via e-mail o SMS, stai in guardia!
2. Controlla gli indirizzi e il linguaggio: I truffatori spesso usano indirizzi email strani e hanno una grammatica disastrosa.
3. Attiva l'autenticazione a due fattori: Così, anche se qualcuno riesce a rubare le tue credenziali, avrà bisogno di un codice che solo tu puoi avere.
4. Contatta direttamente l'ente: Se ricevi una comunicazione strana, contatta sempre l'ente direttamente usando i numeri ufficiali.

Ricorda, prevenire è meglio che curare! Mantieni i tuoi dati al sicuro e fai attenzione a chi dai accesso alle tue informazioni. Con un po' di accortezza, puoi navigare il mondo digitale senza brutte sorprese!



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

L'Inganno con il Viso di Nostro Familiare

Immagina di ricevere, un giorno come tanti, un messaggio sul tuo smartphone che ti lascia senza parole. Un video inquietante appare sullo schermo, e la prima cosa che noti è il viso di tuo figlio o nipote. Sembra stia vivendo un incubo; è in difficoltà, circondato da estranei che gridano e ridono di lui. Il tuo cuore si ferma, l'ansia ti attanaglia lo stomaco.

Non sei solo. Negli ultimi mesi, le truffe alimentate dall'intelligenza artificiale sono aumentate a dismisura. Tecnologie avanzate consentono di manipolare immagini e suoni, creando situazioni così realistiche da sembrare vere. Eppure, ciò che stai guardando non è altro che un'ingiusta simulazione, una distorsione della realtà orchestrata da malintenzionati.

I criminali informatici hanno capito come ingannare le famiglie, gli anziani approfittando della nostra vulnerabilità emotiva. Utilizzano software di deepfake per creare video o foto in cui i volti dei familiari vengono sovrapposti a scene allarmanti. Il loro obiettivo? Estorcere denaro o informazioni sensibili, mentre le vittime si trovano intrappolate in una spirale di paura e panico. Ma non lasciarti sopraffare. La cosa più importante è mantenere la calma. Verifica sempre le informazioni prima di reagire. Contatta direttamente tuo figlio o chiunque conosca per confermare che stia bene. Ricorda, la verità può essere facilmente distorta in un mondo dominato dalla tecnologia.

In questo contesto, è fondamentale riconoscere i segnali di allerta e come difendersi da queste truffe. Solo così possiamo sperare di ridurre il numero di famiglie colpite da questo orribile inganno.

In un mondo in cui nulla sembra più sicuro, la consapevolezza è la nostra migliore arma. agisci, informati e condividi queste esperienze. Solo così possiamo costruire una comunità più forte e resiliente, capace di fronteggiare le sfide del futuro. E nel dubbio **chiama il 112.**



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

Giochi e Quiz e Test on line

Nel vasto e affascinante mondo dei giochi online, dove la competizione si mescola con il divertimento, si annida un'ombra insidiosa: **le truffe.** Questo universo virtuale, che promette avventure straordinarie e ricompense incredibili, attira milioni di giocatori, molti dei quali ignari dei rischi che corrono. Spesso sono test virali su Facebook, Instagram o siti apparentemente innocui. Ti chiedono accesso ai tuoi profili o ti portano su pagine che imitano siti ufficiali.

Si presentano sotto forma di **quiz, giochi o test della personalità**, e

spesso hanno come **obiettivo:**

1. **Raccogliere dati personali (nome, età, e-mail, posizione, ecc.).**
2. **Farti cliccare su pubblicità ingannevoli o link truffaldini.**
3. **Iscriverti inconsapevolmente a servizi a pagamento.**
4. **Rubarti informazioni per usi illeciti (accessi ai social, account vari).**

Esempi comuni:

- **"Scopri chi ti ama in segreto!"**
- **"Che tipo di personalità hai? Rispondi a 5 domande per scoprirlo!"**
- **"Che animale sei nella tua vita passata?"**
- **"Guarda cosa succede se metti il tuo nome!"**

Come riconoscere una truffa travestita da test/gioco:

- **Non fidarti di link condivisi su social o app di messaggistica;**
  Controlla l'URL: è un dominio ufficiale o uno strano sito pieno di pubblicità?
- **Non inserire dati personali sensibili per test banali;**
  Evita di accettare accessi con Facebook o Google se non sei sicuro, del sito;
  Diffida se alla fine chiedono il numero di telefono o la carta di credito;
  Blocca e segnala pagine che sembrano sospette.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

Se hai anche un solo dubbio non esitare a chiamare il

NUMERO UNICO EUROPEO PER LE EMERGENZE





© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

Truffa del finto lavoro

Le **finte offerte di lavoro online** sono una delle truffe più diffuse negli ultimi anni. Si presentano come annunci attraenti, spesso con stipendi alti, poca esperienza richiesta, e possibilità di lavorare da casa. In realtà, servono per **rubare dati personali**, **farti pagare** per "corsi" o "attivazioni", o **coinvolgerti in attività illegali** come riciclaggio di denaro.

1. **Come riconoscere una truffa da finta offerta di lavoro:**

2. **Promettono guadagni altissimi e facili**
   "Guadagna 3000€ (tremila) al mese lavori 2 ore al giorno da casa!"

3. **Non chiedono qualifiche o esperienza**
   "Non serve CV, ti prendiamo subito!"

4. **Ti contattano via WhatsApp, Telegram o email personale**
   Spesso con messaggi mal scritti o generici.

5. **Chiedono soldi in anticipo**
   "Versa 50€ per attivare l'account di lavoro"
   "Devi acquistare il kit iniziale"

6. **Vogliono dati sensibili troppo in fretta**
   Codice fiscale, documento d'identità, numero di conto.

7. **Il sito web è strano o poco professionale**
   Controlla se ha errori, se manca una sede legale o una partita IVA.

8. **Propongono "compiti" ambigui o sospetti**
   Come ricevere bonifici e girarli ad altri (riciclaggio!).

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

1. Esempi di truffe comuni:

- **"Lavoro come mystery shopper"** che richiede pagamento iniziale.
- **"Lavoro in Amazon o Poste Italiane"** ma da e-mail non ufficiali.
- **"Inserimento dati o pacchi"** dove in realtà vogliono il tuo IBAN.
- **Truffe via Telegram/WhatsApp** dove ti chiedono di fare click su link di "registrazione".

2. **Come proteggerti**

- Verifica sempre l’azienda su Google o LinkedIn.
- Non inviare mai soldi per ottenere un lavoro.
- Usa solo portali affidabili come LinkedIn, InfoJobs, Indeed, ecc..
- Se ti contatta qualcuno, chiedi **sede, partita IVA e contratto scritto.**
- Segnala truffe a **Polizia Postale**: https://www.commissariatodips.it

Siate sempre scettici: in un mondo dove il divertimento può trasformarsi in una truffa, la prudenza è il miglior alleato. Giocare è bello, ma farlo in sicurezza è ancora meglio!

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Il finto CUP**

A volte tutto inizia con una telefonata o un messaggio che sembra arrivare dal servizio sanitario, con un tono urgente che parla di una visita o di una prenotazione da confermare e invita a richiamare subito un numero.

La parola “urgente” basta spesso a far scattare la fretta, soprattutto se si sta aspettando una risposta, e si richiama senza pensarci troppo.

Dall’altra parte però non c’è un operatore sanitario, ma una linea che resta in attesa con messaggi o musiche mentre la chiamata continua e il credito si consuma. Anche pochi minuti possono trasformarsi in una perdita senza che arrivi mai una risposta reale.

Funziona perché colpisce nel momento della fretta, quando si agisce prima di verificare.

Per questo la regola è semplice: **non chiamare mai il numero indicato nel messaggio o nella telefonata.** Per qualsiasi verifica usa sempre e solo i canali ufficiali del servizio sanitario, come il sito istituzionale, il CUP della tua ASL o il medico di base.

Se hai già chiamato, contatta il tuo operatore telefonico per controllare eventuali servizi a pagamento e disattivarli.

Se hai comunicato dati personali, password, PIN o inviato documenti, agisci subito: interrompi ogni contatto, segnala l’accaduto al **112** per assistenza.

Gli esperti consigliano di chiamare il proprio operatore e far disattivare la Vas. Il passo successivo è un modulo di reclamo al CoReCom (Comitato regionale per le Comunicazioni, organo funzionale ad Agcom)

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0



Se hai anche un solo dubbio non esitare a chiamare il

NUMERO UNICO EUROPEO PER LE EMERGENZE 112

Puoi utilizzare il portale ufficiale **Commissariato di PS Online**, compilando il modulo nella sezione "Segnala Online"

Lo SPID “invisibile”

Immagina di usare il tuo SPID come fai ogni giorno, per entrare nei servizi online, controllare i tuoi dati, verificare una comunicazione o magari aspettare un rimborso, senza che nulla sembri fuori posto, perché tutto funziona esattamente come sempre.

È proprio questa normalità che fa abbassare l’attenzione, perché non c’è niente che faccia pensare che qualcosa sia cambiato.

Eppure, in alcuni casi, qualcuno potrebbe essere riuscito a utilizzare i tuoi dati personali per attivare un secondo SPID a tuo nome, mentre il tuo continua a funzionare senza problemi e senza dare alcun segnale.

Due identità digitali, che non si vedono tra loro.

E attraverso quell’accesso parallelo è possibile entrare nei portali ufficiali, consultare informazioni e, in alcune situazioni, arrivare anche a modificare dati sensibili come l’IBAN, con la conseguenza che eventuali pagamenti possono prendere una strada diversa da quella prevista.

La particolarità di questa situazione è che non succede nulla di evidente nell’immediato, perché tutto continua a funzionare normalmente, senza avvisi o segnali chiari, fino al momento in cui qualcosa non torna, magari proprio quando un pagamento atteso non arriva.

Ed è spesso solo lì che ci si accorge che qualcosa è cambiato.

Per questo, ogni tanto, è importante fare un passo indietro e rientrare nei propri dati, accedendo direttamente ai portali ufficiali come INPS o NoiPA, verificando che tutto sia coerente con quello che si conosce, senza affidarsi a comunicazioni ricevute o a notifiche inattese.

Allo stesso tempo è fondamentale non condividere mai documenti personali o informazioni sensibili in risposta a richieste improvvise, anche quando sembrano credibili.

Perché in questi casi tutto si gioca su un dettaglio molto semplice: dall’esterno non sembra accadere nulla.

E quando il dubbio si fa sentire, anche solo per un attimo, è già il momento di fermarsi, verificare con calma e intervenire subito se qualcosa non torna.

Parlane con familiari o persone di fiducia, prenditi il tempo di controllare i tuoi dati e, se qualcosa non torna, non aspettare: verifica subito e segnala l’accaduto.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **Il finto Carabiniere / Finanziere / Poliziotto**

In passato queste telefonate iniziavano quasi sempre allo stesso modo: un figlio, un nipote o un familiare coinvolto in un incidente, un problema improvviso, la richiesta urgente di soldi da consegnare subito per risolvere tutto.
Oggi, invece, il racconto cambia forma e spesso sembra ancora più credibile.
Il telefono squilla e dall'altra parte una voce si presenta con sicurezza, dice di essere un Carabiniere, un finanziere o un poliziotto, e parla di una rapina, di un problema legale, di un bonifico urgente da bloccare o di un episodio che riguarderebbe la tua auto o quella di un familiare, mentre tu cerchi ancora di capire e la conversazione continua già oltre, come se alcuni passaggi fossero dati per scontati.
A volte la storia cambia ancora e tutto parte dal presunto ritrovamento di un documento, di una tessera o di un oggetto smarrito, con la richiesta di confermare dati personali che, in quel momento, sembrano normali da comunicare.
La voce resta calma, accompagna ogni spiegazione senza alzare mai il tono, fino a quando arriva la richiesta di controllare soldi o gioielli, di prepararli perché qualcuno passerà a verificarli, come se fosse una procedura normale da svolgere senza perdere tempo.
Ed è proprio mentre tutto sembra scorrere senza interruzioni che qualcosa, anche solo per un attimo, inizia a non combaciare più del tutto.
Perché, al di là della storia raccontata, queste situazioni fanno quasi sempre leva sulle stesse cose: la fretta, la fiducia, l'autorità e la paura di sbagliare proprio in quel momento.
E spesso basta proprio quel dubbio per interrompere la chiamata, prendere distanza da quella situazione e riportare tutto fuori da quella pressione che fino a poco prima sembrava plausibile.
A quel punto verificare torna a essere qualcosa che si fa con calma, usando un altro telefono o aspettando qualche minuto, e se qualcuno si presenta alla porta è importante restare all'interno, senza aprire.
Perché nessuna urgenza arriva così.
E quando qualcosa non convince, anche solo per un momento, è già il momento di fermarsi, parlarne con qualcuno di fiducia e segnalare quanto accaduto. Chiama il 112.



© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme Siamo più Forti”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/

Borseggiatori con il POS: realtà o esagerazione?

Immagina di essere in mezzo alla folla, sul bus, al mercato o in fila al supermercato, in uno di quei momenti in cui le persone si muovono continuamente e il contatto tra sconosciuti diventa normale, quasi inevitabile, al punto che non ci fai più caso.
Qualcuno si avvicina più del solito, sfiora il tuo fianco o lo zaino, e per un attimo tutto si perde dentro quella confusione fatta di spazi stretti e movimenti continui.
Poi ti torna in mente qualcosa sentito tempo fa, la possibilità che esistano dispositivi in grado di effettuare pagamenti semplicemente avvicinandosi a una carta contactless, e da quel momento inizi quasi senza accorgertene a guardarti intorno in modo diverso.
Negli ultimi tempi si è parlato dei cosiddetti borseggiatori con il POS, persone che utilizzerebbero terminali portatili per tentare pagamenti avvicinandosi alle vittime.
L'idea colpisce proprio perché sembra qualcosa che può avvenire senza farsi notare.
Eppure, nella realtà, serve una condizione molto precisa, perché il dispositivo dovrebbe trovarsi praticamente a contatto con la carta e senza ostacoli, mentre nella vita quotidiana la carta è quasi sempre dentro un portafoglio, in una tasca o in una borsa, e questo rende tutto molto più difficile.
Per questo motivo, situazioni di questo tipo restano poco probabili, mentre molto più spesso il rischio reale è quello che si conosce da sempre, un portafoglio sfilato, uno zaino aperto, un attimo di distrazione in mezzo alla folla.
Ed è proprio lì che conviene riportare l'attenzione.
Controlla sempre dove tieni le carte, evita tasche esterne o zaini aperti, attiva le notifiche dei pagamenti e, se noti anche una sola operazione che non riconosci, non aspettare: contatta subito la banca e blocca la carta.
Perché alla fine non è tanto lo scenario a fare la differenza, ma il tempo con cui si reagisce.
E se qualcosa non torna, anche solo per un attimo, verifica subito, parlane con qualcuno di fiducia e non esitare a segnalare.



Se hai anche un solo dubbio non esitare a chiamare il

NUMERO UNICO EUROPEO PER LE EMERGENZE



- **L’assicurazione troppo conveniente**

Sempre più spesso si cercano assicurazioni online, magari in un momento qualsiasi della giornata, quando si ha un attimo libero e si prova a capire se esiste un modo per risparmiare senza rinunciare a nulla.
Tra i siti che compaiono, ce ne sono alcuni che sembrano subito familiari, con colori già visti, loghi riconoscibili e parole che danno una sensazione di sicurezza, come se si fosse già nel posto giusto senza bisogno di fermarsi davvero a controllare. Si inserisce la targa quasi senza pensarci e in pochi secondi compare un’offerta che attira più delle altre, perché promette la stessa copertura a un prezzo molto più basso, ma solo per un tempo limitato, come se fosse un’occasione da cogliere subito prima che sparisca.
Ci si ferma un attimo a guardarla, mentre prende forma l’idea che possa essere davvero un buon affare, e proprio in quel momento può arrivare anche una telefonata, con una voce calma che accompagna la scelta senza forzare, ma lasciando intendere che aspettare troppo potrebbe far perdere quell’opportunità. Subito dopo arriva un messaggio con un contratto, dei documenti e un link per completare tutto: ogni elemento sembra al suo posto, senza sospetti evidenti, e così si procede perché tutto è costruito per sembrare normale.
Passano i giorni, ma non arriva nulla: nessuna conferma, nessun documento valido, nessuna risposta. Il numero non è più raggiungibile e il sito, tornando a cercarlo, non esiste più.
Ed è solo in quel momento che diventa chiaro che quel percorso era stato costruito nei dettagli per portare proprio lì, senza lasciare segnali evidenti lungo la strada. Per questo, prima di arrivare fino in fondo, basta fermarsi un attimo e verificare da un punto esterno, attraverso i canali ufficiali o contattando direttamente l’IVASS al numero verde 800 486661.
E se qualcosa non torna, anche solo per una sensazione, è già il momento di fermarsi e chiedere un confronto a qualcuno di fiducia.
Parlane con familiari o amici, verifica sempre prima di pagare e, se temi di essere stato raggirato, segnala subito l’accaduto.



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

- **La polizza vita “sicura”**

Sempre più spesso capita di essere contattati con proposte che parlano di sicurezza e protezione, soprattutto quando riguardano i risparmi costruiti nel tempo e il desiderio di metterli al riparo da qualsiasi imprevisto.

La voce dall’altra parte si presenta con calma, senza fretta, con un modo di parlare che non mette pressione ma accompagna, e descrive una soluzione che sembra pensata proprio per dare tranquillità, una polizza che protegge e fa crescere il denaro senza esporlo a rischi.

Le parole scorrono in modo lineare, senza creare dubbi immediati, e nei giorni successivi arrivano anche documenti, tabelle, riferimenti a una compagnia conosciuta, elementi che danno continuità a quella prima impressione, come se tutto seguisse un percorso già tracciato.

Si ascolta, si valuta, e a un certo punto la scelta sembra naturale, quasi una conseguenza di quello che è stato detto e mostrato, così si firma, si paga, e per un breve periodo sembra che tutto proceda.

Poi, lentamente, qualcosa cambia.

Le comunicazioni si interrompono, il numero non risponde più e, quando si prova a verificare, emerge ciò che prima non era visibile: quella polizza non esiste, quella proposta non è mai stata reale.

Solo allora si ricompone il quadro, e si capisce che ogni passaggio era stato costruito per arrivare fin lì, senza mai creare un momento evidente in cui fermarsi.

Per questo, prima di arrivare a quel punto, è importante fare un passo fuori da quel percorso e verificare attraverso i canali ufficiali, controllando sempre che l’intermediario e la compagnia siano autorizzati o contattando direttamente l’IVASS al numero verde 800 486661, perché spesso è proprio questo controllo a cambiare completamente la direzione.

E quando il dubbio si fa sentire, anche solo per un attimo, è già il momento di fermarsi, non procedere e confrontarsi con qualcuno di fiducia.

Parlane con familiari o amici, verifica sempre prima di pagare e, se temi di essere stato raggirato, segnala subito l’accaduto.

Se hai anche un solo dubbio non esitare a chiamare il

NUMERO UNICO EUROPEO PER LE EMERGENZE



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

RICORDA SEMPRE CHE:

- Nessun ufficio pubblico o privato (INPS, INAIL, ASL, ecc.) invia propri dipendenti a domicilio per riscuotere pagamenti, verificare bollette o controllare banconote e gioielli.

- Nessuna azienda fornitrice di luce, gas o acqua chiede informazioni su denaro o gioielli.

- Nessun addetto alla consegna di plichi, raccomandate o altra corrispondenza si reca sul pianerottolo di casa: la consegna avviene al portone, nell'androne del palazzo oppure nella cassetta postale.

- Se ti contattano sostenendo che un tuo figlio o parente è in pericolo (ad esempio in ospedale, coinvolto in un incidente o in arresto) e ti chiedono denaro o gioielli per aiutarlo, **non fidarti**: anche se la voce sembra familiare, potrebbe trattarsi di un truffatore.

- Se si presentano sconosciuti alla porta o citofonano dichiarando di appartenere alle Forze dell'Ordine, oppure indossano divise e mostrano tesserini, berretti o palette con simboli ufficiali, **non aprire**. Controlla dal balcone o dalla finestra se in strada è presente una vettura di servizio e cerca di capire il motivo della visita.

- Se ti chiedono di entrare in casa per controllare l'impianto elettrico, del gas o dell'acqua, o per effettuare riparazioni, **non aprire** se non hai ricevuto una comunicazione ufficiale dalla società erogatrice del servizio. Controlla sempre la presenza di un mezzo aziendale all'esterno e, in caso di dubbio, contatta direttamente la società.

- Non utilizzare numeri di telefono forniti da sconosciuti, anche se dicono di voler dimostrare la loro identità.

• Non fornire mai informazioni personali a persone che non conosci. Se ti accorgi di averle condivise con un truffatore, **denuncia subito** per proteggere la tua identità.

Per la tua sicurezza online

Se usi l'home banking dal tuo smartphone, proteggi sempre i tuoi dati. Ti consiglio di usare una casella e-mail dedicata solo alle comunicazioni bancarie, diversa da quella principale.

Quando accedi a Internet, connettiti sempre tramite una VPN sicura, evita le reti Wi-Fi pubbliche e fai attenzione ai QR code che scansioni.

• se sei vittima di una truffa, racconta quanto accaduto ai tuoi amici e familiari. Eviterai che a loro volta siano truffati.

CHIAMA SEMPRE IL

NUMERO UNICO EUROPEO PER LE EMERGENZE



© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

RINGRAZIAMENTI

Un ringraziamento particolare alle persone che mi hanno supportato nella realizzazione di questo vademecum:

alla Segretaria Gen. Stefania Castricone, e alla Segreteria del Si.Na.Fi.

(Sindacato Nazionale Finanzieri) per il gratuito patrocinio;

al Christian Diana Direttore Generale della "Anglo American Academy" di Cagliari, per il gratuito patrocinio;

al Dr. Antonio Pirro Agente Generale dell'Agenzia Generali Cagliari Porto per il gratuito patrocinio;

all'artista Francesco Mascia Cogoni e all'amico Luca Meloni per le splendide illustrazioni realizzate con Microsoft Designer, Gemini, Flow, Chatgpt;

al Dr. Roberto Borghetti e al Dott. Matteo Capaldo del Gruppo Trizio;

al Dr. Gennaro Fuoco per il tempo dedicatomi;

all'amico Luca Agati per la costante fiducia;

al Dr. Alberto Covini per il suo amichevole supporto*.*

Alle Officine Grafiche della Sardegna S.r.l. – (CA) per la sensibilità dimostrata.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

Sicurezza degli account online: una protezione che non va mai sottovalutata

Oggi usiamo Internet per molte cose importanti.
Con poche semplici attenzioni è possibile proteggere meglio i propri account.

● **Usare password sicure**
La password dovrebbe essere lunga e difficile da indovinare.
È importante usare password diverse per ogni servizio.

Per esempio:
la password della banca non dovrebbe essere la stessa dell'email o dei social.

● **Attivare il controllo con codice**
Molti siti, oltre alla password, chiedono anche un codice ricevuto sul telefono. Questo aiuta a proteggere l'account anche se qualcuno scopre la password.

● **Tenere aggiornati telefono ed email di recupero**
Numero di telefono ed email devono essere sempre corretti e funzionanti.
Servono per recuperare l'account se si perde la password o non si riesce più a entrare.

● **Conservare i codici di emergenza**
Alcuni servizi danno codici speciali da conservare in un posto sicuro.
Possono aiutare a rientrare nell'account in caso di problemi.

● **Usare strumenti di protezione aggiuntivi**
Esistono app o piccoli dispositivi che aumentano la sicurezza degli account.

Tutte queste protezioni devono essere controllate ogni tanto.
Anche un vecchio numero di telefono non più usato può creare problemi nel recupero dell'account.

La sicurezza online dipende da tante piccole attenzioni che, insieme, aiutano a proteggere dati e informazioni personali.

se sei vittima di una truffa, racconta quanto accaduto ai tuoi amici e familiari. Eviterai che a loro volta siano truffati.

Inoltre desidero esprimere una particolare menzione e un sentito riconoscimento a **"Striscia la Notizia"** e a tutti i suoi collaboratori e inviati. Grazie al loro instancabile impegno e alla dedizione con cui affrontano tematiche rilevanti e attuali, il programma si distingue per il fondamentale ruolo di vigilanza che esercita nei confronti delle truffe, sia sul territorio che nel mondo digitale.

Le rubriche non solo informano il pubblico sulle insidie più comuni, ma forniscono anche consigli pratici su come prevenire potenziali raggiri. In un'epoca in cui le frodi assumono nuove forme e metodologie sempre più sofisticate, la capacità di "Striscia la Notizia" di portare alla luce queste problematiche rappresenta un servizio prezioso per la comunità.

Attraverso un linguaggio accessibile e reportage incisivi, il programma guida i cittadini verso una maggiore consapevolezza e una migliore preparazione contro le truffe. È grazie a questi sforzi che molti possono sentirsi più al sicuro e protetti, sapendo di poter contare su un'informazione chiara e diretta.

© Cavoli Sergio 2025 – CC BY-NC-ND 4.0

GRATUITO PATROCINIO OFFERTO DA

© Cavoli Sergio 2025 – “Vademecum contro le Truffe: Insieme Siamo più Forti”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso consentito: citare l’autore, non modificare, non usare a fini commerciali.
Link alla licenza: https://creativecommons.org/licenses/by-nc-nd/4.0/