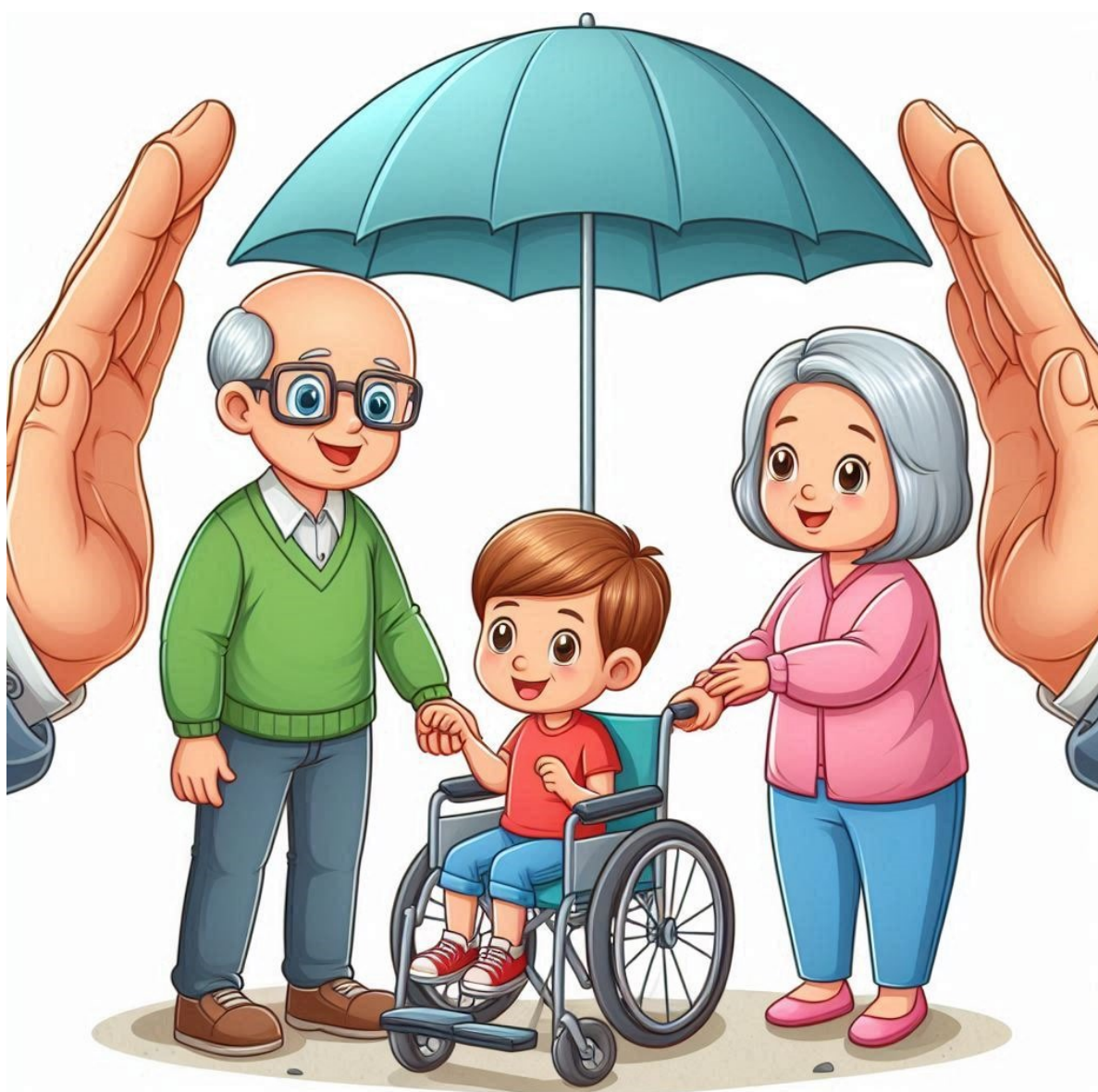


HANDBOOK AGAINST FRAUD

TOGETHER WE ARE STRONGER



CONTENTS

FOREWORD	p. 05
I. THE RECIPIENTS	p. 07
II. THE FRAUDSTERS	p. 09
III. AT HOME	p. 11
a. FALSE FRIENDS	p. 14
b. THE FAKE COURIER	p. 17
c. THE FAKE INSURANCE AGENT	p. 19
d. THE FAKE LAWYER OR LAW ENFORCEMENT OFFICER	p. 21
e. HOW TO PROTECT YOUR HOME	p. 25
IV. ON THE ROAD	
a. IN THE SUPERMARKET PARKING LOT	p. 31
b. NEAR THE BANK OR POST OFFICE	p. 33
c. IN THE PARK OR ON THE STREET	
• One push too many	p. 35
• The hug scam	p. 37
• Faking illness	p. 39
• Magicians and holy men	p. 41

© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

www.infotruffe.com

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

d.	AT THE MARKET AND AMONG THE STALLS	
•	The bag trick	p. 43
•	The jacket trick	p. 45
•	The fake greengrocer trick	p. 47
•	The detour	p. 49
•	The circle	p. 51
•	Two minutes	p. 53
V.	BY BICYCLE	p. 55
VI.	ON PUBLIC TRANSPORT	p. 57
VII.	BY CAR	
•	Driving	p. 59
•	Parking	
•	The plastic bottle and money on the windscreen	p. 63
VIII.	IN PUBLIC PLACES	p. 65
IX.	COMPUTER FRAUD	p. 66
•	<i>Man in the middle</i>	p. 69
•	Online trading scams	p. 71
•	<i>Cryptolocker</i>	p. 73
•	<i>Digital extortion</i>	p. 73
•	Romantic scam	p. 75
•	<i>Sex extortion</i>	p. 77

• <i>The evolution of triple extortion</i>	p. 79
• Tips for buying and selling items on the Internet	p. 81
• The fake inheritance	p. 83
• PAYPAL payments	p. 83
• Prize / lotteries winnings	p. 83
• <i>Phishing</i>	p. 85
• <i>Vishing</i>	p. 87
• <i>Smishing</i>	p. 87
• <i>Pharming</i>	p. 87
• <i>Trojan</i>	p. 89
• <i>Fake Crowdfunding</i>	p. 91
• The scam with the face of a family member	p. 93
• Quiz games and Test on-line	p. 95
• Fake job scam	p. 99
• The fake booking service	p.103
• The invisible SPID	p. 105
• The fake policeman	p. 107
• Pickpockets with POS	p. 109
• Insurance that's too good to be true	p. 111
• The "secure" life insurance policy	p. 113
• Always remember	p. 115
• thanksgiving	p. 117
• Online Account Security	p- 119

INTRODUCTION

In these pages, I have compiled a list of situations that are unfortunately becoming increasingly common, exposing elderly and vulnerable people to scams by unscrupulous criminals.

This is a constantly growing phenomenon, a real social emergency that is often underestimated or treated too lightly.

My name is Sergio Cavoli and I am a pensioner. For many years, I have been actively involved in supporting vulnerable people, particularly those who, like me, live with multiple sclerosis.

For over a year, I have been engaged in a complex personal battle against cancer, an experience that has reinforced in me the value of solidarity, sharing, and mutual aid.

This journey led to the book *Passi di Speranza* (Steps of Hope), a testimony of courage and resilience that recounts how, even in the hardest of trials, it is possible to transform suffering into an opportunity for growth and service to others.

In the same spirit, the Handbook Against Scams Targeting the Elderly and Vulnerable has now been created. It is a practical, clear, and easily accessible tool, designed to be kept at home and shared with anyone who may need it.

The Handbook contains over forty examples of real or plausible attempts at fraud, which increasingly target the elderly and vulnerable.

It is divided into three main sections:

Home scams, Street scams, and Computer scams, and aims to:

- raise awareness and provide information on the main types of scams currently in circulation;
- provide practical advice on how to recognize warning signs and react promptly;
- promote a culture of prevention and shared security as a fundamental tool for personal and collective protection.

With the right information and a few simple precautions, we can all learn to protect ourselves and our loved ones.

Let's always remember that prevention is our best defense.

And if, despite everything, you do fall victim to a scam, there is no need to be ashamed: talking to someone you trust and promptly contacting the police is the first step in reacting and protecting yourself.

Only through awareness, collaboration, and mutual support can we truly protect those who are most vulnerable.

Together we can make a difference.

Together we can face and overcome any obstacle.

Together we can turn difficulties into strength.

REMEMBER THE SINGLE EUROPEAN EMERGENCY NUMBER



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

www.infotruffe.com

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

I. THE RECIPIENTS

The worrying increase in scams, especially those targeting elderly and vulnerable people, has made this guide necessary. It is designed to provide practical advice on prevention.

Those who are most vulnerable—due to age, health, or living conditions—are often prime targets for scammers and thieves. Many live alone, have limited mobility or chronic illnesses, and sometimes keep cash or valuables at home because they do not trust banks or post offices. All these factors increase the risk of being scammed or robbed.

It is essential to remember that fragility is not only a matter of age: it also concerns health, social isolation, and emotional difficulties. The homes of these people become easy targets for those who take advantage of their trust or carelessness, also because they do not always have confidence.

Prevention is possible. In these pages, you will find simple and immediate advice on how to recognize dangers, avoid risky behavior, and know who to turn to in case of need.

Safety comes from awareness and cooperation.

The police forces — the Carabinieri, the State Police, the Guardia di Finanza, and the Fire Department — ensure the control of the territory every day.

In case of doubt or suspicious situations, always call

THE SINGLE EUROPEAN EMERGENCY NUMBER



Protecting the most vulnerable is everyone's duty.



THE SCAMMERS

Scammers can take many forms and operate in various contexts. We live in a society where appearances can be deceiving, and unfortunately there are individuals who exploit vulnerability to carry out scams and deception. In this guide, we outline some of the most common types:

- Street fraudsters: they operate physically, on the street or by coming to your door, staging desperate situations to rob you or sell goods, often fake, at bargain prices.
- Online scammers: they exploit the internet to perpetrate fraud, such as phishing, where they try to obtain personal information by pretending to be trustworthy entities;
- Telephone scammers: they use telephone calls to deceive people, sometimes posing as public officials or company representatives.



I. AT HOME

DO NOT OPEN THE DOOR: A CALL TO BE VIGILANT

In recent years, we have seen a worrying increase in scams perpetrated by individuals posing as law enforcement officers or authorised workers.

Wearing a uniform or presenting an ID card may seem like a sign of legitimacy, but it is not always synonymous with truth. Criminals are becoming increasingly cunning and skilled at creating false documents and imitating the appearance of agents or professionals in the sector to gain the trust of their victims.

The excuse for entering the home can vary: from the alleged need to check for water leaks to more serious dangers such as gas leaks. Once inside, the result is almost always the same: theft and looting.

Fraudsters can disguise themselves under various identities:

- Post office officials
- Charity workers
- Representatives of the National Insurance Institute (INPS), the local council or electricity, water and gas companies
- People who claim to be law enforcement officers.

Always friendly and well dressed, they try to convey a sense of reassurance. However, their kindness could hide malicious intent.



Before opening the door:

1. Do not open the door immediately: if you have any doubts, it is always better to keep the door closed and communicate through a peephole or window.
2. Do not trust immediately: even if they seem like respectable, decent people, remember that appearances can often be deceiving.
3. Check their identity: if someone presents themselves as a law enforcement officer, ask them to identify themselves. Law enforcement officers do not normally operate alone and are always in uniform, almost never in plain clothes.
4. Check first that there is a service car parked nearby.
5. Do not hesitate and do not be afraid to ask the reason for the visit. Real officers are used to providing clear and detailed explanations.

It is essential to remember that, in case of doubt, it is always advisable to contact the relevant authorities to verify the identity of those knocking on the door.

Do not hesitate to ask for information and, if necessary, request the intervention of real officers. CALL 112.

Elderly and vulnerable people should be educated to recognise these scams.

Families must play an active role in informing their loved ones about these types of risks and preventive strategies.

a. FALSE FRIENDS

They may show up at your house as friends of a relative or acquaintance. Imagine you are at home, surrounded by the aroma of freshly brewed coffee. It is a moment of tranquillity, a moment of relaxation that you have allowed yourself after a long day. But that moment of peace can easily turn into something else if, suddenly, you hear a knock at the door. In an age where security seems increasingly precarious, it is essential to pay attention to who we are dealing with when it comes to opening our door. Let's imagine that “friends” of relatives or acquaintances show up at the door. “Hello, I'm a friend of Marco's!” they might say. Or: 'Hello, I've come on behalf of Francesca.' These phrases, often uttered with a reassuring smile, may seem harmless, but they represent potential risks.

These “false friends” know exactly how to weave a web of trust in a matter of seconds to gain access to your private spaces and can use the names of trusted individuals to break down barriers of mistrust. In such cases, it is essential to remain vigilant and thoughtful.

The first rule to follow is therefore not to open the door.

There are numerous reasons why this decision is crucial:

- 1. Home security:** your home is your refuge and you must not compromise its security in any way. Statistics on burglaries and scams show that many of these situations begin with an apparent ‘twist’ rooted in the simplicity of a friendly greeting.

2. Identification: Before letting someone into your home, it is wise to verify their identity. First, ask, 'Who are you? What do you want?' You can also make a quick phone call to the relative or friend in question to confirm their identity.

3. The Empathy Trap: People tend to trust strangers if they appear vulnerable. 'I need help' or 'Please, just give me a few quid' are phrases that can tug at our heartstrings. But empathy, if not accompanied by a critical assessment of the situation, can lead us to make rash decisions.

If you find yourself in a similar situation, you need to be prepared. Here are some tips on how to deal with the situation without opening the door:

- If someone knocks on your door, do not be afraid to answer from inside. Ask questions and listen carefully to the answers. Remember: you have the right to protect your privacy and safety.
- Use security devices: Today, many of us have video cameras or smart doorbells. These tools not only allow you to see who is at the door, but can also act as deterrents to potential scammers.
- Do not give in to pressure: If you feel drawn in by someone else's narrative, remember to stay calm. Even if their words seem persuasive, your safety is worth much more. If, unfortunately, you find yourself in a situation where a scammer has made contact with you, stay clear-headed. Never provide money or personal information. Write down any recognisable details and **Call 112**.

Sharing stories and warnings about scam attempts can build a collective safety net. If you know of other cases in your area or someone trying to defraud your acquaintances, alerting others is an act of civic responsibility.



b. THE FAKE COURIER

It is not uncommon for a courier to arrive at your door asking for payment for the delivery of a parcel. These individuals claim that the goods were ordered by your children, relatives or other people in your building.

1. If you receive a delivery notice, make sure that the recipients are actually aware of the order. Contact them before proceeding.
2. Do not accept unexpected parcels: if you have not been given any prior information about this parcel, do not accept it.
3. Do not make any payments before receiving confirmation. If the courier seems insistent, **CALL 112**.

If you have any doubts or suspicions, please call the





c. THE FAKE INSURANCE AGENT

In recent years, rising insurance prices have made many consumers vulnerable to misleading offers. It is not uncommon, therefore, to encounter a self-proclaimed insurance agent knocking on your door or approaching you near an ATM inside a shopping centre. With a charming smile and persuasive words, these individuals offer insurance policies for your family, car or home at extremely competitive prices.

The temptation to save money is strong, and in times of economic crisis, many people can fall into the trap. After a long conversation and some tempting promises, the crucial moment arrives: payment. With some haste, the agent has you sign documents that look official and hands you a piece of paper, apparently an insurance policy. However, you may be surprised to discover that this document has no legal value.

Disillusionment quickly turns to concern: you have just spent money on something completely useless. It is therefore essential to be careful and wary of offers that seem too good to be true. Before signing any policy, it is advisable to do your research, check the agent's credentials and compare genuine offers on the market. Caution is key to protecting not only your wallet, but also your peace of mind. **CALL 112.**



d. THE FAKE LAWYER OR LAW ENFORCEMENT

It is certainly a distressing situation: receiving a phone call from a solicitor, police officer, finance officer or hospital switchboard informing you that your child or grandchild has had a serious accident and is in hospital, or has been arrested and urgently needs financial help. Such news is devastating and can immediately cause fear and anxiety. However, it is essential to remain calm and know how to recognise if it is a scam.

Scammers take advantage of strong emotions, creating urgent and dramatic scenarios to force you to react impulsively. Often, they ask you to send money immediately or accompany them to an ATM to withdraw large sums of money.

Do not act on instinct: take time to reflect and analyse the situation.

However, there are some warning signs to look out for:

1. Urgent requests for money.
2. No confirmation: if you are not given any verifiable details about the alleged accident or legal problem, be suspicious.
3. Uncertainty about the details: they may be vague about the facts, the location of the accident or the nature of the arrest.

please call the

THE SINGLE EUROPEAN EMERGENCY NUMBER





What should you do if you receive such a call?

- Do not respond impulsively: take a moment to think and verify the authenticity of the call.
- Contact your family member directly: call your child or grandchild to confirm the situation. If you cannot reach them, speak to other family members or friends.
- Do not let anyone in: if a supposed “accomplice” of the fraudsters shows up at your home, do not open the door. Do not be persuaded to hand over money or follow them under any circumstances.
- Encourage other family members and friends to recognise these warning signs and to remain sceptical about urgent requests for money. Being informed is the first step in protecting yourself against these scams.

Remaining vigilant and precise is essential. Remember: when in doubt, always check!

If you suspect you are the victim of a scam, **call 112**. Any useful information can help stop the scammers.



e. HOW TO PROTECT YOUR HOME

Living in a secure home is everyone's dream, and with a few simple precautions, our home can be just that. Burglars prefer isolated, quiet homes with no barriers.

The following may be useful:

- mutual cooperation between neighbours, to stay in touch if necessary, so that there will always be someone to check on your home during your absence, whether short or long;
- always lock the entrance door to the building;
- hide your house keys in safe and well-hidden places;
- do not open the front door or the door to your home unless you are sure of the identity of the person knocking;
- Install a security door with a digital peephole.
- Do not leave personal documents in easily accessible places.
- Install burglar alarms and/or video surveillance devices. Always activate the alarm every time you leave the house and, if possible, even when you go to sleep. Today, there are tax breaks for this type of installation.
- Do not attach name and address tags to your key ring, as these could easily identify your flat if lost.
- Pay particular attention to lighting the entrance and dark areas.
- Install window bars or shatterproof glass if you live on a low floor or in a detached house. Today, there are tax breaks for these measures.





- If If you live in an isolated house or, if you have the opportunity, consider adopting a dog.

A dog is not only a loyal companion and source of affection, but also a valuable ally in home security: its presence and barking can deter intruders, while caring for it increases vigilance, awareness of the surrounding environment, and a feeling of protection, regardless of which floor you live on.



- When you go on holiday, do not post photos or information on social networks. You can do so only when you return. Inform only your loved ones of your absence. If your trip or work will keep you away from home for a long time, it is always best to ask a family member or trusted friend to check on your home from time to time.
- If you are going away for the weekend, or if you are home alone and do not have a security system, leave a light or the radio on to show and make it seem to outsiders that the house is occupied. Today's burglars are mainly looking for money, so it may be useful to leave a few large banknotes with a note saying: "There is no other money in the house and no jewellery, please do not cause any damage".

Once inside, burglars try to go to the bedroom first and then move on to less obvious places. From wardrobes to clothes, toilet cisterns, sofa cushions, sugar jars, vases and pictures, every nook and cranny will be explored.

- When you return home, if you notice that the lock has been tampered with, the door is ajar, or the shutters have been broken, do not enter the house; call 112. Similarly, if you notice that you have been burgled as soon as you enter your home, do not touch anything and call immediately

THE SINGLE EUROPEAN EMERGENCY NUMBER





If you have any doubts or suspicions, please call the

112

II. ON THE ROAD

a. IN THE SUPERMARKET CAR PARK

- When leaving supermarkets, we often encounter people offering to help us push our trolleys or carry our shopping bags to our cars or homes. This gesture of kindness seems harmless and even courteous, but behind this service lies a much more disturbing reality.
- It is essential to be cautious and aware that, in some cases, these individuals may have malicious intentions. Their goal is not only to lighten the load of our bags, but also to gather as much information about us as possible.
- They may offer to accompany us to the post office, bank or even the cash machine to pick up crucial details about our daily habits, the places we frequent and, in some cases, personal information about our accounts and savings. A smile and a kind gesture can mask less noble intentions.
- It is therefore important to always remain vigilant and protect your personal data, because the information collected could be used to rob you at a later date!

THE SINGLE EUROPEAN EMERGENCY NUMBER





b. NEAR THE BANK OR POST OFFICE

If someone approaches you, especially after you have withdrawn cash from a bank or post office, be careful! These individuals often present themselves as bank or post office employees, claiming, for example, that they need to check the serial numbers on your banknotes because they may be counterfeit.

Remember: no bank or post office employee will ever stop you or come to your home to check your banknotes! This is a well-known scam. The criminal's goal is simple: to obtain your legitimate money by replacing it with counterfeit banknotes or seizing it completely.

Never hand over your money: if someone asks you to do so, stay calm and do not give in. **If you are still on the street, attract the attention of passers-by and CALL 112.**



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

a. IN A PARK or ON THE STREET

- **One push too many.**

Imagine you are sipping a coffee or a cold drink, watching a group of children playing, for example. Someone with a pram or a woman out jogging accidentally bumps into you, knocking over your drink and spilling it on you. 'I'm so sorry!' they exclaim, as they rush to offer help, with a caring look. But here's the trick: as they bend down to clean up the mess they've created, their hand quickly moves towards your rucksack or bag.

In a matter of seconds, they manage to steal your wallet, mobile phone or even your house keys, and walk away with the excuse that they dropped something. Not only can this scheme be orchestrated by women with children, but also by men who take advantage of the situation. Imagine a young man who, with a friendly smile, approaches you to ask for information. Perhaps it is a well-thought-out trick: while he distracts you with conversation, an accomplice loiters near your bag, ready to seize the moment. The alarming thing is that these theft tactics happen too quickly, while the victims, unaware and trusting, believe they are dealing with well-meaning people. Sharing family moments and the friendly environment can make it difficult to perceive the imminent danger. Therefore, it is essential to remain vigilant even in the most innocuous places. It is important to protect your belongings and your safety without leaving room for opportunists.

It is never wrong to be cautious. Even in moments of apparent normality, there may be hidden dangers ready to catch you off guard.

Awareness is the best defence against these criminals. If you have unfortunately been the victim of one of these scams, call 112 immediately.



- **The hug scam**

The deception of illusion: young women and the trap of scams.

In recent years, we have witnessed an increasingly worrying phenomenon involving young women and older men. These interactions, which appear harmless or even flattering on the surface, often conceal malicious intentions. Young women, with their kind and charming attitude, approach more mature men, creating the illusion of an emotional or seductive connection. This dynamic can be seen as a form of deception that exploits the vulnerability of the elderly. The interaction begins with compliments and affectionate behaviour. Women often use sweet phrases and friendly gestures, making their victims feel special and important. This approach can mislead the elderly, leading them to believe that there is genuine romantic or sexual interest. When the elderly person, perhaps hopeful of embarking on a game of seduction, rejects the advances, the situation takes an unexpected turn. At this point, these women have no scruples: they continue to show affection, approaching for a hug that might seem harmless. However, at that very moment, the real twist takes place: their skilled and quick hands move stealthily to take away wallets, mobile phones or watches. The victim, caught off guard, finds themselves taken aback, confused and, often, powerless in the face of such a devious act. This type of fraud not only has material consequences for the elderly person who has been robbed, but also leaves deep emotional scars. Trust is broken and a sense of security vanishes, giving way to mistrust that can negatively affect future interactions. It is therefore essential to raise awareness of this issue and encourage people, especially the most vulnerable, to maintain a critical and cautious approach towards new acquaintances. If you are a victim of this type of scam, do not hesitate: **CALL 112.**



- **The feigned illness**

On the crowded streets of the city, you may encounter situations that, at first glance, seem to require your intervention. Sometimes a person may feign illness by collapsing to the ground with the desperate air of someone in need of help. Our instinct is to approach them and try to understand how we can assist someone who appears to be in difficulty. However, it is essential to remain vigilant and aware. In these situations, the reality may be quite different. The illness may be just a pretence, a clever deception orchestrated by criminals. As you approach to offer assistance, an accomplice – blending into the crowd – may strike. In a moment of distraction, you find yourself calling for help, watching an ambulance that never arrives, while the thief crouching next to you grabs your bag or wallet and disappears into the surrounding chaos. Unfortunately, this type of scam is more common than you might think. It is not just a question of a lack of empathy or kindness; it is important to protect not only our own well-being, but also that of others. So what should you do in these situations?

- Observe carefully. If you notice someone who appears to be in difficulty, assess the situation calmly.
- Do not approach immediately; try to see if there are other people around, if the person is already receiving assistance from someone else.
- Call the emergency services.

Remember that your act of altruism is commendable, but caution must always guide your actions. Never underestimate the possibility of deception. Being attentive and cautious can protect you from unpleasant surprises and ensure that your help really goes where it is needed.



- **Magicians and holy men**

Even today, despite living in a modern and advanced society, it is surprising how widespread the phenomenon of magicians and holy men can be. These figures, often gifted with charisma and persuasive abilities, manage to capture the attention of vulnerable people, exploiting their desperation. Those facing serious health problems or work difficulties may be tempted to seek alternative, often illusory, solutions.

Many of these “professors” of the occult offer miraculous promises: quick cures for incurable diseases, solutions to financial problems or even luck in love. However, behind such claims lies a much more bitter reality: the manipulation of human emotions for profit. People, especially the elderly, in their search for help, fall victim to these scams and end up spending considerable sums of money on rituals and practices that have no scientific basis.

In Italy, practising as a magician is prohibited. The law punishes the practice of pseudoscience, recognising the right of citizens to receive valid care and support based on concrete evidence. It is essential to remember that, for any problem, it is always advisable to consult qualified professionals: doctors, psychologists and specialists. Only by relying on these figures can you obtain accurate diagnoses and appropriate treatment, avoiding falling into the traps of those who exploit the fragility of others.

Do not hesitate, **CALL 112.**



- **The bag trick.**

Among the stalls, you may be attracted by a small display of handmade bags. As soon as you approach, the salesperson invites you to try one on. While the salesperson pretends to be distracted, you notice that inside there is, for example, a wallet full of banknotes. Without hesitation, you buy the bag, trying not to attract the salesperson's attention. As soon as you walk away from the stall, your curiosity to discover the treasure is too great, but you find that what looked like banknotes are pieces of scrap paper!

THE SINGLE EUROPEAN EMERGENCY NUMBER





- **The jacket trick.**

Your gaze falls on a stall displaying jackets. Intrigued, you approach and the seller invites you to try one on. As you put on the jacket, you feel an object in the pocket and find, for example, a sparkling watch. 'A Rolex! Incredible!' you think. You buy the jacket without thinking twice. There is something thrilling about the idea of owning a piece of clothing that comes with a valuable watch. A few moments later, as you walk away with your new jacket, you open the pocket.

That bargain that seemed so advantageous turns out to be an illusion: the watch was a well-made fake, but still a fake. And the jacket? It wasn't even worth half the price you paid.

Both experiences teach a valuable lesson. The temptation of an unmissable bargain can cause us to lose our clarity of mind. It's easy to get caught up in the excitement of the moment, but it's essential to remain vigilant and cautious.

Street stalls can offer unexpected treasures, but also deceptions disguised as opportunities. The world is full of scammers ready to exploit people's naivety.



- **The fake greengrocer trick.**

Near markets or city parks, it is easy to come across a scene that arouses sympathy and compassion: a man, with a sad expression and teary eyes, approaches you. His trembling voice tells a heartbreaking story: he lost his job to stay with his sick wife or son in serious condition. He tells you about the unsustainable healthcare costs, the desperate need for help and how he decided to sell fruit or vegetables to try to cope with the emergencies.

The image of a family in difficulty touches the deepest chords of your soul. He offers you the goods, presenting them as fresh and of excellent quality. Without thinking too much about it, you decide to help him, paying a price well above the real value of those products. You watch him load the fruit or vegetables into your boot, with an expression of gratitude that seems sincere.

But when you get home, you realise that although the fruit and vegetables look nice and fresh, they are actually poor quality. You can call 112 because it is not just a matter of fraud, but a necessary step to stop those who exploit people's good faith.

THE SINGLE EUROPEAN EMERGENCY NUMBER





- The detour

You're in a crowded station, the buzz of people fills the air, trains arrive and depart non-stop, voices mingle, some people stop, others run, and you have only one direction in mind: an exit to reach amidst that constant flow.

At some point, a person approaches you naturally, as if it were perfectly normal to speak to you there amidst all that chaos, and tells you that one side is completely closed, that there's no point in carrying on like this and that it's better to go the other way – quicker, easier – and they say it with a calm confidence, without hesitation.

And without there really being a moment when you ask yourself why, you find yourself following them.

At first, nothing changes; the station is still the same, the familiar noises, the movements around you, everything seems normal, but as you walk, something slowly begins to shift; the crowd thins out without you really noticing, the sounds fade, the passages become narrower, and the route changes without any clear sign.

Then comes that feeling that's hard to explain, as if the landmarks you had before are no longer the same, as if you're moving forward but without fully recognising the direction, and yet you keep walking because by now you're on that path and turning back isn't as straightforward as it seemed at the start.

And that is precisely where everything can still be stopped.

Pause for a moment, without rushing, as if you were simply catching your breath; look around and take in your surroundings, and if something doesn't sit right with you or no longer seems clear, don't carry on out of habit: say goodbye naturally, thank them, and head back to a place you know.

If you feel uncertain or uneasy, don't stay alone with that feeling. Approach other people, stay in busier areas, or ask for help from those nearby, because the presence of others immediately changes your perception of what you're experiencing.

And if something doesn't feel right, even for just a moment, it's already time to stop and, if in doubt, call 112.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

The circle

You're at a bus stop, in a park or queuing somewhere – one of those moments when you're simply waiting and the people around you keep moving without you really noticing.

Sometimes someone approaches with a phone or headphones and says, "Let me play you something"; other times it's a simple question, a piece of information, something that seems harmless and normal, and in both cases you stop without thinking too much about it, because it's a situation that seems part of everyday life.

And it is precisely whilst you are there, with your attention on that person, that the scene changes without any obvious transition.

Other people arrive, four or five of them, almost silently, and within seconds they get too close, creating a closed space around you whilst everything happens quickly and in a coordinated manner: hands move swiftly, bags are opened, pockets are rummaged through, whilst your attention is still fixed on that initial moment.

By the time you try to react and realise something is wrong, the group has already dispersed; everyone walks off in a different direction, blending into the crowd as if nothing had ever happened.

And that is precisely where everything happens in a matter of seconds.

Don't stand there trying to work out straight away what has happened: it creates distance. Move decisively away from the initial encounter and head towards a more open, busy area.

If someone still tries to speak to you or hold you back, don't stop to argue: a brief reply, whilst you keep moving, such as "I'm sorry, I have to go", is more than enough.

Immediately look for a safe spot, a familiar face, a shop, a group of people – anything that brings you back into a clear and controllable situation – and only then, calmly, assess what has happened.

Share what happened with family and friends, because recognising these patterns helps to avoid them.

And if something doesn't feel right, don't wait: call 112.



Two Minutes

You're on a street, at a station, or in a square, surrounded by the constant flow of people, when someone walks past you, leaves a backpack or a package near you, and casually says, "Hold this for a second," as if it were the most natural thing in the world, and without giving you time to reply, they're already disappearing into the crowd.

You stand there with that object beside you, in a situation that has unfolded in just a few moments while everything around you keeps moving.

Shortly after, another person arrives; their gaze falls first on the object and then on you, and simple yet persistent questions begin: whether it's yours, what's inside, why it's there—as if, in some way, you were already caught up in a situation that's taking shape.

And as you try to answer, all attention focuses on that spot, while the rest around you keeps flowing but loses importance, becoming background.

And that's exactly where everything plays out in a matter of seconds.

The important thing is not to get caught up in it: immediately take a step back, walk away calmly, leave the object where it is, and move toward a more open space or toward other people, where the situation breaks up and everything becomes clearer.

If someone insists or tries to hold you back, don't stop to explain: say a short phrase, without slowing your pace, such as "it's not mine, I don't know anything about it," and keep walking away.

And if you have even the slightest doubt or feel in trouble, don't hesitate to call 112.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

III. BY BICYCLE

When deciding to travel by bicycle, it is essential to pay attention not only to personal safety, but also to the safety of your belongings. A common mistake that many cyclists make is to store bags or bum bags in the front basket of their bicycle. Although this may seem like a convenient and practical solution, there are several reasons why it is advisable to avoid this habit.

Firstly, the basket is easily accessible to both the cyclist and any potential thieves. Leaving valuables in plain sight greatly increases the risk of theft. Even if you only leave your bike unattended for a moment, an experienced thief could take advantage of this to quickly snatch your bag or bum bag without being noticed.

Secondly, placing heavy or bulky items in the basket can compromise your balance. An unbalanced load can make the bicycle difficult to manoeuvre, increasing the risk of falls or accidents. Safety while cycling should always be a priority.

Finally, another aspect to consider is the protection of your belongings. An open basket offers no protection against the elements. If it rains or is windy, your personal effects could be damaged.

The ideal solution is therefore to use a specially designed bicycle bag, which can be mounted on the frame or on your back.

In summary, when travelling by bicycle, it is best to avoid storing bags or bum bags in the basket. Opt for safer alternatives and keep your belongings protected so you can enjoy your ride with peace of mind.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

IV. ON PUBLIC TRANSPORT

When travelling by bus or underground, the safety of your personal belongings becomes a key priority. Public transport, while an efficient way to get around the city, can also be a breeding ground for theft and distraction.

That's why it's essential to take certain preventive measures:

- Keep your wallet in your front trouser pocket, as this significantly reduces the risk of theft and allows you to keep an eye on it at all times, avoiding having to rummage through bags or rucksacks every time you need to pay for a ticket or show your ID.
- Carry your bag in front of you, across your chest. Carrying your bag across your body or in a central position not only makes it more difficult for a thief to sneak up on you, but also allows you to have greater visibility of what is happening around you. In crowds, it is best to be aware of any suspicious movements and, at the same time, protect your belongings more effectively.
- Choosing bags with secure zips and multiple pockets can help you organise your personal belongings better, making it more difficult for thieves to access everything at once.
- Using durable materials and less conspicuous colours can also help you keep a low profile, avoiding drawing attention to your valuables.
- Always remain vigilant and pay attention to your surroundings. Being aware of your space and the people around you can make the difference between a peaceful journey and a stressful experience. With a little care and caution, you can enjoy the benefits of public transport without taking any risks.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

V. IN THE CAR

- **Driving.**

When travelling by car, it is essential to take certain precautions to ensure your safety and that of your belongings. One aspect that is often overlooked is never leaving bags or bum bags on the passenger seat, especially with the window open. This situation is an invitation to thieves, as it makes theft easier.

At traffic lights or in traffic jams, your attention may be focused on other things, and if someone approaches your car, with a quick and discreet gesture, your bag can be stolen without you even noticing. Unfortunately, this scenario is more common than you might think.

To avoid these situations, get into the habit of keeping your windows up and your doors locked, especially when you are in crowded or unsavoury areas. Not only will you protect your personal belongings, but you will also feel safer inside your vehicle.

This habit can make a huge difference in preventing car theft.

If you hit another vehicle or pedestrian while driving and the driver gets out and shows damage to the bodywork of their car, or the pedestrian complains of being hit on the leg, they may ask you to settle amicably with a small amount of cash. In such cases, the wisest thing to do is to stay in your car and immediately call 112 to report the incident, providing useful details about the location and the identity of the people involved. To protect yourself in situations like this, you may want to consider purchasing a dash cam (dashboard camera). Today, they are available at affordable prices and can record everything that happens while you are driving.

These cameras can provide valuable evidence in the event of accidents or attempted fraud, giving you peace of mind and safety on the roads.

SINGLE EUROPEAN EMERGENCY NUMBER



- **Parked.**

If you are sitting in your car waiting for someone, always lock the doors, and if someone approaches you for information, never roll down the window and wait for that person to walk away. They could be a potential criminal. Personal safety must always come before any casual interaction: in today's world, caution must become an integral part of our daily lives.

**please call the
SINGLE EUROPEAN EMERGENCY NUMBER**



Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



- **The plastic bottle and money on the windscreen.**

The thieves, targeting a specific vehicle, place an empty plastic bottle in the front tyre of the car. This manoeuvre is particularly sneaky, as the driver rarely notices the foreign object stuck in the wheel. When the driver starts the engine, the noise made by the crushed bottle attracts their attention. The concerned motorist gets out of the car to check what is happening. It is at this moment that the thieves spring into action: taking advantage of the situation, often with the engine running and the keys in the ignition, they drive off with the vehicle in a matter of seconds, leaving the rightful owner incredulous and helpless. The success of this scam is in line with other fraudulent techniques, such as the sticker scam or the flat tyre scam, all characteristic of an era in which carelessness can be costly. Even when we are in a hurry, it is crucial to pay particular attention to our car before driving off, focusing on the tyres and checking for any suspicious details. A small detail, even if not apparent, could be a warning sign. Even an empty shopping trolley behind our car should alarm us, as should a banknote, usually €10 or €20, placed on the windscreen. In any case, the only precaution to take is not to get out of the car, but to walk away quickly. If this is not possible, it is important to make sure that all the doors are locked and immediately call 112, sounding the horn to attract the attention of passers-by or other motorists.

Remembering these simple steps can make a big difference. Prevention is essential in combating this type of crime. In a context where car theft is on the rise, information and awareness can be your main allies in avoiding becoming a victim of ingenious scams such as those described above.



VI. IN PUBLIC PLACES

When eating out, it is essential to pay attention not only to the food, but also to the safety of your personal belongings. Here are some practical tips to avoid theft or loss that can ruin your evening:

1. Do not leave your bag unattended. It is common practice to place your bag on the armrest of your chair, thinking it is safe. However, this practice can expose your belongings to theft. It is preferable to keep your bag safe at all times, perhaps by placing it between your legs or using a specific bag hook, if available at the table and in any case purchasable for € 5 (five).
2. Be careful with your jacket: another common mistake we make is to leave our jacket on the back of the chair, along with valuable items such as our wallet. Nothing could be easier for a thief than to grab your jacket and run away or rummage through it. If you need to take off your jacket, consider hanging it on a coat rack or keeping it on your lap.
3. Be careful with your smartphone: never leave it on the table. Smartphones are one of the most sought-after items by thieves. Today, they are the key to our lives, and not everyone knows how to lock them and render them unusable. Leaving it on the table may seem convenient, but it provides the perfect opportunity for anyone who wants to steal it. It is better to keep it in your jacket or trouser pocket.

Always keep an eye on your personal belongings and enjoy your evening with peace of mind!



VII. COMPUTER FRAUD

Today, with the internet, criminals no longer have a face and... they never sleep.

All it takes is one click, made without realising it, for them to enter our homes and our lives.

Online dangers can come in many forms and with varying levels of risk.

Do not be afraid or ashamed.

If you have any doubts or feel in difficulty, ask for help and call 112.

SINGLE EUROPEAN EMERGENCY NUMBER





© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- ***Man In The Middle***

A prime example of this illegal activity is called man-in-the-middle, whose main objective is to steal our information. It is a form of attack directed at routers or servers in which a third party, the attacker, intercepts and alters the communication between two parties who believe they are communicating with each other. For example, they position themselves between the victim and the server (as in the case of an online banking or email server). These attacks are effective and difficult to detect.

As a first line of defence, avoid using free Wi-Fi networks, especially if you plan to carry out sensitive transactions. It would be better to use a browser plug-in that can establish secure connections.

Do not visit websites when your browser alerts you to a problem with their security certificate.

If the web page you are visiting has started downloading files automatically, without your permission, this site is almost certainly compromised.

Always update your antivirus software, preferably choosing one that has an internal web page control system that informs the user when they are about to enter a dangerous site.

Finally, it would be preferable to have a dedicated computer for transactions only.



- **Online trading scams.**

Even in this world, there is no shortage of scams, so always be wary of anyone offering easy money. Investing in the stock market can be tempting, and we would like to make our savings grow through online trading.

Online trading can be done from the comfort of your own home and computer and consists of buying and selling financial securities remotely. It is a risky activity because you earn on the difference in price between the purchase and sale of shares and bonds. You cannot operate directly on the financial markets. You need to use a financial broker, i.e. an intermediary who buys and sells securities on behalf of the client. The fraudster contacts the unsuspecting victim, most often through a fake call centre, under the pretext of offering easy investment solutions with large profits. Although hesitant, we may be tempted to entrust small sums of money, which will be returned quickly with the first profits. At that point, the criminals will ask for a larger sum with the false promise of a guaranteed return, and once they have received the requested amount, the fake trading operator will disappear, leaving the victim unable to recover what they have apparently invested.

To trade and avoid scams, CONSOB has made a platform of authorised brokers available to users.

If you have any doubts, contact CONSOB on 06.8477611 (Monday to Friday, from 9.00 to 13.00 and from 14.30 to 16.30) and report it.



- ***Cryptolocker:***

It is a Trojan virus that first appeared in 2013 and was perfected in 2017. This malware is a form of ransomware that infects Windows systems and encrypts the victim's data, demanding payment, a ransom, for decryption. To date, about 3% of those affected by this malware decide to pay. Some victims report that, despite paying the ransom, they have not seen their files decrypted. Do not pay, but report it!

- ***Digital Extortion:***

This term refers to activities carried out by cybercriminals with the aim of extorting money from individuals or companies in exchange for not disclosing data from emails, pornographic websites visited or other compromising material (stolen using ransomware) that could damage a person's image and social relationships. Anyone can fall victim to a digital extortion attack, from private citizens to celebrities to politicians and companies. Do not open suspicious emails or download unknown files.

If you have any doubts or suspicions, please call the





- **Romantic Scam:**

The scammer carefully chooses victims on various social media platforms (Facebook, Instagram, Telegram, etc.), creates fake profiles on dating sites and apps, creates a plausible story and posts frequently so that their profile appears real (the images and photos on the fake profile are taken from the internet). The scammer is not looking for sex; conversations are always friendly. They establish a relationship with you to build trust and emotional dependence, so it will be easier to ask for money for sudden financial difficulties or to buy a ticket to join you. This ploy works because it plays on the need to feel loved and valued. Unfortunately, this type of scam has been on the rise in recent years, but you should report it and notify the social networking site or app where you encountered the scammer.

SINGLE EUROPEAN EMERGENCY NUMBER





- ***Sex Extortion:***

Sextortion is a serious crime that occurs when someone threatens to distribute private and sensitive material unless they are provided with sexual images, sexual favours or money.

Online predators may gain your trust by pretending to be someone they are not. They also lurk in chat rooms and record people who post or stream sexually explicit images and videos of themselves, or they may hack into your electronic devices using malware to access your files and control your webcam and microphone without you knowing.

- Never send compromising images of yourself to anyone, no matter who they are or who they say they are.
- Do not open attachments from people you do not know.
- Turn off your electronic devices and webcams when you are not using them.
- If you are being blackmailed, do not pay; cut off all contact and report it immediately.

Help us find these criminals and stop them from ruining people's lives.

SINGLE EUROPEAN EMERGENCY NUMBER





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

It is the latest evolution of the previous one: criminals encrypt data and exfiltrate it, threatening to leak it if ransom demands are not met. If a victim refuses to pay, the stolen data can be auctioned off on cybercrime forums. This gives criminals another way to monetise their illegal actions. But they have gone even further with triple extortion schemes. In some cases, they encrypt and steal data, threaten a company's employees, contact family members and company managers, and overload websites with traffic (also known as DDoS or Distributed Denial-of-Service attacks) to force payment. Sometimes a Trojan is hidden in the threat message received.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

www.infotruffe.com

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- **Tips for buying and selling items on websites:**

It is impossible for the police to monitor all e-commerce websites, in addition to the widespread use of buying and selling apps that offer products at attractive prices. This is why fraudsters find fertile ground and can easily take advantage of it to deceive buyers by offering non-existent or counterfeit products.

In addition to this phenomenon, the victim of the scam is the person selling their goods. They are contacted by the fraudster who, pretending to be a potential buyer, is almost always a resident of another city or outside Italy: these individuals actually want to steal personal data in order to perpetrate other scams.

- Be wary of anyone offering a product at a price that is too cheap.
- Be wary if the buyer is located abroad.
- Check for the padlock symbol for secure transactions at the top right of the website and always use a secure payment method (NO Western Union, gift cards, top-ups, etc.).
- Do not enter personal information to redeem a voucher or unlock a fictitious discount.
- Do not download any software to complete the purchase.
- Never pay money in advance for suspicious customs operations, expenses and commissions.
- Check the company's details (VAT number, registered office).

Always be wary if the cost of the item you want to buy is significantly lower than that offered on official websites.



- **The fake inheritance.**

Who has never wished for a rich unknown relative to leave them a large inheritance? Be careful, you may be contacted by a lawyer or notary because you are the recipient of a large inheritance, but in order to receive it, you will have to pay a certain amount to a person appointed by the notary.

The TV program “Striscia la Notizia” has documented several similar cases across Europe.

Never pay money in advance when you are the one who is supposed to receive it. Any such request is absolutely not legitimate, so always report it.

- **Payment PAYPAL:**

Do you use PayPal for your purchases? Fine, but if you make a payment with a description that is not relevant to the transaction, such as “**send payment/send gift to friends and family,**” and your purchase is not successful, **please note that you will not be able to make any claims.**

PayPal does not protect purchases unless they are transactions for goods or services.

- **Prize / lotteries winnings**

SMS/WhatsApp messages asking you to pay a small administrative fee in exchange for wonderful prizes, trips, or resort stays are becoming increasingly common: these are usually scams. After paying the requested amount via bank transfer, gift card, or cryptocurrency (secure payment systems for criminals), you will receive nothing.

Do not send money to anyone you do not know. Receiving a prize is free of charge. I am sorry to disappoint you, but you have encountered a scammer.



- ***Phishing:***

It is a type of scam carried out on the Internet through which a malicious person tries to deceive the victim by convincing them to provide personal information, financial data, or access codes, pretending to be a trustworthy entity in a digital communication.

The term phishing is a variant of fishing and refers to the use of increasingly sophisticated techniques to “fish” for a user's financial data and passwords.

Generally, the victim receives a notification of unusual activity on their bank account via email or fake text message. These emails and text messages contain a link that redirects you to a clone of the bank's website. Once you enter the requested data, the scammer has full access to your bank account.

Always pay attention to the following signs that can help you spot phishing scams: No bank would ever send you a direct link to your online current account or to a page where you can enter your personal and banking details. It is best to be wary of such communications and, if in doubt, check with your bank's customer service centre.

- Many phishing messages are poorly written and may contain spelling, typing, and grammar errors.
- Fraudulent emails and messages will most likely direct you to an unsafe website, so always check the URL and the spelling of the company name.
- Do not open emails that contain attachments, as they may contain viruses that will infect your device.



- ***Vishing:***

It is a scam similar to phishing, exploiting the greater trust people have in human contact, but the aim is the same: to deceitfully obtain private information over the phone. The operator asks the victim to provide their details, such as their username and PIN. It is advisable to end the call immediately.

- ***Smishing:***

Smishing differs from phishing in that it uses convincing text messages to trick recipients into sending the requested private information or downloading malicious programs onto their PC or smartphone via a link in the message.

- ***Pharming:***

A cyberattack aimed at stealing personal data. The scammer directs the victim to a “clone” website with an official domain name designed to steal the victim's personal data or install malware on the user's computer in order to obtain personal and financial information.

This type of attack is very difficult to detect, as cybercriminals attack the DNS (Domain Name Server) and use it to redirect users to a fake website.

**If you have any doubts or suspicions, please call the
SINGLE EUROPEAN EMERGENCY NUMBER.**



- **Trojan:**

The term “Trojan” refers to remote access malware that is installed on the victim's computer. Malware is divided into dozens of subcategories (Trojan-Proxy, Keylogger Trojans, Trojan-Spy, etc.) with a single common denominator: stealing sensitive data stored on computers.

Trojans do not spread independently; often it is the victim themselves who unwittingly downloads a Trojan onto their computer by not paying attention to the emails they receive or the websites they visit. Recently, Trojan viruses have been identified in files with the PDF extension.



- ***Fake Crowdfunding:***

Crowdfunding is simply a fundraising initiative generally launched to deal with medical emergencies, including those following earthquakes or floods, or to finance individuals, foundations, or associations in order to carry out worthy projects. The scam involves three parties: the donor, the recipient, and the perpetrator. The latter retransmits or alters communications between the two parties; specifically, they divert the funds to their own bank account held at foreign banks. This scam is often preceded by Trojan or phishing attacks. These cyber attacks, whether they come from an email, phone call, or text message, masquerade as official communications from a government agency or major company and have a common goal: to deceive the recipient in order to extort sensitive data and gain access to bank accounts and credit cards.

Here are some tips to avoid this:

1. Never trust suspicious requests: If someone asks you for personal information via email or text message, be on your guard!
2. Check addresses and language: Scammers often use strange email addresses and have terrible grammar.
3. Enable two-factor authentication: That way, even if someone manages to steal your credentials, they will need a code that only you can have.
4. Contact the organization directly: If you receive a strange communication, always contact the organization directly using the official numbers.

Remember, prevention is better than cure! Keep your data safe and be careful who you give access to your information. With a little caution, you can navigate the digital world without any nasty surprises!



- **The scam with the face of a family member**

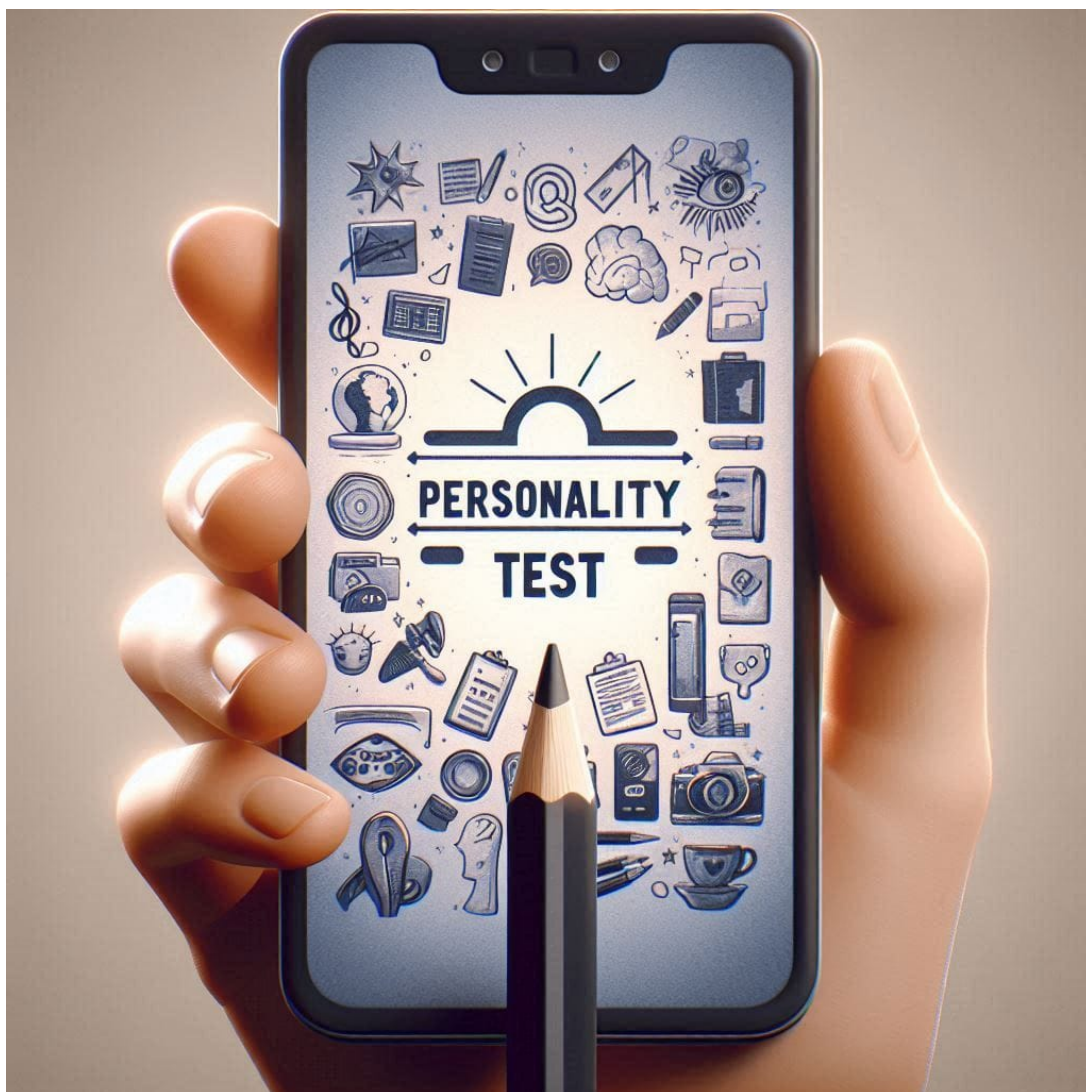
Imagine receiving a message on your smartphone one day that leaves you speechless. A disturbing video appears on the screen, and the first thing you notice is the face of your child or grandchild. They seem to be living a nightmare; they are in distress, surrounded by strangers who are shouting and laughing at them. Your heart stops, anxiety grips your stomach.

You are not alone. In recent months, AI-powered scams have skyrocketed. Advanced technologies allow images and sounds to be manipulated, creating situations so realistic that they seem true. Yet what you are watching is nothing more than an unfair simulation, a distortion of reality orchestrated by malicious individuals.

Cybercriminals have figured out how to deceive families and the elderly by taking advantage of our emotional vulnerability. They use deepfake software to create videos or photos in which the faces of family members are superimposed on alarming scenes. Their goal? To extort money or sensitive information, while their victims are trapped in a spiral of fear and panic. But don't let yourself be overwhelmed. The most important thing is to stay calm. Always verify the information before reacting. Contact your child or anyone you know directly to confirm that they are okay. Remember, the truth can be easily distorted in a world dominated by technology.

In this context, it is essential to recognize the warning signs and how to defend yourself against these scams. Only then can we hope to reduce the number of families affected by this horrible deception.

In a world where nothing seems safe anymore, awareness is our best weapon. Take action, stay informed, and share these experiences. Only then can we build a stronger and more resilient community, capable of facing the challenges of the future. **And when in doubt, call 112.**



- **Quiz games and Test on-line**

In the vast and fascinating world of online gaming, where competition mixes with fun, there lurks an insidious shadow: scams. This virtual universe, which promises extraordinary adventures and incredible rewards, attracts millions of players, many of whom are unaware of the risks they run. Often these are viral tests on Facebook, Instagram, or seemingly harmless websites. They ask for access to your profiles or take you to pages that mimic official sites.

They come in the form of quizzes, games, or personality tests, and often have the following objectives:

1. Collect personal data (name, age, email, location, etc.).
2. Get you to click on misleading advertisements or fraudulent links.
3. Unwittingly sign you up for paid services.
4. Steal your information for illegal use (access to social media, various accounts).

Common examples:

- “Find out who secretly loves you!”
- “What kind of personality do you have? Answer 5 questions to find out!”
- “What animal were you in your past life?”
- “See what happens when you enter your name!”

How to recognize a scam disguised as a test/game:

- Do not trust links shared on social media or messaging apps;
- Check the URL: is it an official domain or a strange site full of advertisements?
- Do not enter sensitive personal data for trivial tests;
- Avoid logging in with Facebook or Google if you are unsure about the site;
- Be wary if they ask for your phone number or credit card details at the end;
- Block and report pages that look suspicious.

**If you have any doubts, do not hesitate to call
the
SINGLE EUROPEAN EMERGENCY NUMBER.**





- **Fake job scam**

Fake online job offers are one of the most common scams in recent years. They appear as attractive advertisements, often offering high salaries, little experience required, and the possibility of working from home. In reality, they are used to steal personal data, make you pay for “courses” or “activations,” or involve you in illegal activities such as money laundering.

1. **How to recognize a fake job offer scam**

2. **They promise very high and easy earnings**

“Earn €3,000 (three thousand) per month working 2 hours a day from home!”

3. **They do not ask for qualifications or experience**

“No CV needed, we'll hire you right away!”

4. **They contact you via WhatsApp, Telegram, or personal email**

Often with poorly written or generic messages.

5. **They ask for money in advance**

“Pay €50 (fifty) to activate your work account.”

“You have to buy the starter kit.”

6. **They want sensitive data too quickly**

Tax code, ID, account number.

7. **The website is strange or unprofessional**

Check for errors, missing registered office or VAT number.

8. **They propose ambiguous or suspicious “tasks”**

Such as receiving bank transfers and transferring them to others (money laundering!).



1. Examples of common scams:

- “Work as a mystery shopper” requiring an initial payment.
- “Work at Amazon or the US Postal Service” but from unofficial emails.
- “Data entry or package sorting” where they actually want your bank account number.
- Scams via Telegram/WhatsApp where they ask you to click on a “registration” link.

How to protect yourself

- Always check the company on Google or LinkedIn.
- Never send money to get a job.
- Only use reliable portals such as LinkedIn, InfoJobs, Indeed, etc.
- If someone contacts you, ask for their address, VAT number, and a written contract.
- **Report scams to the Postal Police: <https://www.commissariatodips.it>**

Always be skeptical: in a world where fun can turn into a scam, caution is your best ally. **Playing is fun, but doing so safely is even better!**

SERVIZIO SANITARIO now

URGENTE!
Hai una visita / prenotazione da confermare.
Richiama subito il numero **02 1234567**

! NON RISPONDERE A QUESTO MESSAGGIO

Richiamo subito, potrebbe essere importante...

Numero sconosciuto
Chiamata in corso...

La preghiamo di attendere. La sua chiamata è importante per noi.

€ CREDITO IN DIMINUZIONE

**COSA FARE SEMPRE:
VERIFICA SOLO ATTRAVERSO I CANALI UFFICIALI.**

 SITO ISTITUZIONALE DELLA TUA ASL Visita il sito ufficiale della tua ASL.	 CUP DELLA TUA ASL Chiama il numero ufficiale del CUP.	 MEDICO DI BASE Contatta il tuo medico di base.
--	---	--

**! NON CHIAMARE MAI IL NUMERO INDICATO NEL MESSAGGIO O NELLA TELEFONATA.
LA FRETTA PUÒ COSTARTI CARA.**

- The fake booking service

Sometimes it all starts with a phone call or a text message that appears to come from the health service, with an urgent tone mentioning an appointment or a booking that needs confirming, and urging you to call back a number immediately.

The word 'urgent' is often enough to make you panic, especially if you're waiting for a reply, and you call back without thinking twice.

On the other end, however, there is no healthcare operator, just a line that keeps you on hold with messages or music whilst the call continues and your credit runs out. Even a few minutes can turn into a waste of time without ever receiving a real response.

It works because it strikes at a moment of haste, when you act before checking.

That's why the rule is simple: never call the number given in the message or during the call. For any verification, always use only the official channels of the health service, such as the official website, your local health authority's booking service (CUP) or your GP.

If you have already called, contact your mobile operator to check for any paid services and deactivate them.

If you have disclosed personal details, passwords, PINs or sent documents, act immediately: cut off all contact and report the incident to 112 for assistance.

Experts advise calling your operator to have VAS services deactivated. The next step is to submit a complaint form to CoReCom (Regional Communications Committee, a body under AGCOM).



- The “Invisible” SPID

Imagine using your SPID just as you do every day—to access online services, check your data, verify a message, or perhaps wait for a refund—without anything seeming out of the ordinary, because everything works exactly as it always has.

It is precisely this sense of normality that lulls you into a false sense of security, because there is nothing to suggest that anything has changed.

Yet, in some cases, someone may have managed to use your personal data to activate a second SPID in your name, while yours continues to function without a hitch and without giving any warning.

Two digital identities, unaware of each other.

And through that parallel access, it’s possible to log into official portals, view information, and, in some situations, even modify sensitive data such as your IBAN, with the result that any payments may take a different path than intended.

The peculiarity of this situation is that nothing obvious happens immediately, because everything continues to function normally, without warnings or clear signs, until something doesn’t add up—perhaps precisely when an expected payment fails to arrive.

And it’s often only then that you realize something has changed.

That’s why, every now and then, it’s important to take a step back and review your own data by logging directly into official portals like INPS or NoiPA, verifying that everything matches what you know, without relying on messages you’ve received or unexpected notifications.

At the same time, it is essential never to share personal documents or sensitive information in response to sudden requests, even when they seem credible.

Because in these cases, everything hinges on a very simple detail: from the outside, nothing seems to be happening.

And when doubt creeps in, even for just a moment, it’s already time to stop, check calmly, and take immediate action if something doesn’t add up.

Talk to family members or people you trust, take the time to check your information, and if something doesn’t add up, don’t wait: verify it immediately and report the incident.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

www.infotruffe.com

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- The fake Carabinieri / tax officer / police officer

In the past, these phone calls almost always began in the same way: a son, a grandson or a relative involved in an accident, a sudden problem, an urgent request for money to be handed over immediately to sort everything out.

Today, however, the story takes a different form and often seems even more credible.

The phone rings and a confident voice on the other end introduces itself, claiming to be a Carabinieri, a tax officer or a police officer, and speaks of a robbery, a legal problem, an urgent bank transfer to be blocked or an incident involving your car or that of a family member, whilst you are still trying to make sense of it all and the conversation has already moved on, as if certain details were taken for granted.

Sometimes the story changes again and it all starts with the alleged discovery of a document, a card or a lost item, with a request to confirm personal details which, at that moment, seem perfectly normal to share.

The voice remains calm, accompanying every explanation without ever raising its tone, until the request comes to check money or jewellery, to have them ready because someone will be coming to verify them, as if it were a normal procedure to be carried out without wasting time.

And it is precisely when everything seems to be running smoothly that something, even if only for a moment, starts to feel slightly off.

Because, regardless of the story being told, these situations almost always play on the same things: haste, trust, authority, and the fear of making a mistake at that very moment.

And often that very doubt is enough to hang up the call, step back from the situation and remove everything from that pressure which, until a moment before, seemed plausible.

At that point, verifying the situation becomes something you do calmly, using another phone or waiting a few minutes, and if someone comes to the door, it is important to stay inside without opening it.

Because nothing urgent ever happens like that.

And when something doesn't feel right, even for just a moment, it's already time to stop, talk to someone you trust and report what has happened.

Call 112.



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

www.infotruffe.com

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- Pickpockets with POS devices: reality or exaggeration?

Imagine you're in the middle of a crowd, on the bus, at the market or queuing at the supermarket – one of those moments when people are constantly on the move and contact between strangers becomes normal, almost inevitable, to the point where you no longer even notice it.

Someone gets closer than usual, brushes against your side or your rucksack, and for a moment everything gets lost in that confusion of tight spaces and constant movement.

Then you remember something you heard a while ago – the possibility that there are devices capable of making payments simply by getting close to a contactless card – and from that moment on, almost without realising it, you start looking around in a different way.

Recently, there has been talk of so-called 'POS pickpockets' – people who allegedly use portable terminals to attempt payments by getting close to their victims.

The idea is striking precisely because it seems like something that could happen without being noticed.

Yet, in reality, a very specific condition is required, as the device would need to be practically in contact with the card and unobstructed, whereas in everyday life the card is almost always inside a wallet, in a pocket or in a bag, and this makes the whole thing much more difficult.

For this reason, situations of this kind remain unlikely, whereas the real risk is far more often the one we've always known: a wallet snatched from your hand, an open rucksack, or a moment's distraction in a crowd.

And that is precisely where we need to focus our attention.

Always keep an eye on where you keep your cards, avoid external pockets or open rucksacks, enable payment notifications and, if you notice even a single transaction you don't recognise, don't wait: contact your bank immediately and block your card.

Because ultimately, it's not so much the scenario that makes the difference, but how quickly you react.

And if something seems off, even for just a moment, check it straight away, talk to someone you trust and don't hesitate to report it.



- Insurance that's too good to be true

More and more often, people are looking for insurance online, perhaps at any time of day, when they have a spare moment and try to work out if there's a way to save money without compromising on anything.

Among the many websites that pop up, there are some that immediately seem familiar, with colours you've seen before, recognisable logos and words that give a sense of security, as if you've already found the right place without really needing to stop and check.

You enter your number plate almost without thinking, and within seconds an offer appears that stands out from the rest, because it promises the same cover at a much lower price, but only for a limited time, as if it were a bargain to be snapped up before it disappears.

You pause for a moment to look at it, as the idea takes shape that this might really be a good deal, and just at that moment a phone call might come through, with a calm, professional voice guiding your choice without pressuring you, but hinting that waiting too long could mean missing out on that opportunity.

Immediately afterwards, a message arrives with a contract, some documents and a link to complete the process, and every element seems to be in place, without raising any obvious suspicions, so you proceed, because everything has been designed to look normal.

The days go by, but nothing arrives: no confirmation, no valid documents, no reply; the number can no longer be reached and, when you go back to look for the website, it no longer exists.

And it is only then that it becomes clear that this seemingly straightforward process had been meticulously designed to lead you right there, without leaving any obvious clues along the way.

That is why, before going all the way, it is enough to pause for a moment and step back from that path, checking from an outside perspective, through official channels or by contacting IVASS directly on the freephone number 800 486661, because sometimes it is precisely that small check that completely changes direction.

And if something doesn't add up, even if it's just a feeling that's hard to explain, it's already time to stop, not proceed, and seek advice from someone you trust.

Talk to family or friends, always check before paying, and if you fear you've been scammed, report the incident immediately. Call 112.

FERMATI E VERIFICA PRIMA



**LE OFFERTE CHE PROMETTONO TROPPO
POSSONO COSTARE MOLTO CARE.**

VERIFICA SEMPRE PRIMA DI PAGARE.



Intermediario
autorizzato



Compagnia
regolare



Informazioni
verificate



Scelta consapevole,
futuro più sicuro.

The “secure” life insurance policy

We are increasingly approached with proposals that promise security and protection, particularly when they concern savings built up over time and the desire to safeguard them against any unforeseen events.

The voice on the other end is calm and unhurried, speaking in a way that doesn't pressure but rather guides, and describes a solution that seems designed specifically to provide peace of mind: a policy that protects and grows your money without exposing it to risk.

The words flow smoothly, raising no immediate doubts, and in the days that follow, documents, tables and references to a well-known company arrive – elements that reinforce that first impression, as if everything were following a pre-determined path.

You listen, you weigh things up, and at a certain point the choice seems natural, almost a consequence of what has been said and shown, so you sign, you pay, and for a short while it seems that everything is going according to plan.

Then, slowly, something changes.

Communication breaks down, the number no longer answers, and when you try to check, what was previously invisible comes to light: that policy does not exist, that proposal was never real.

Only then does the picture come together, and you realise that every step had been designed to lead up to that point, without ever creating a clear moment to stop.

For this reason, before reaching that point, it is important to take a step back and verify the details through official channels, always checking that the intermediary and the company are authorised, or by contacting IVASS directly on the freephone number 800 486661, because it is often this very check that completely changes the course of events.

And when doubt creeps in, even for just a moment, it is already time to stop, not proceed, and consult someone you trust.

Talk to family or friends, always check before paying, and if you fear you have been scammed, report the incident immediately.

Call 112.

**If you have any doubts, do not hesitate to call
the
SINGLE EUROPEAN EMERGENCY NUMBER.**



ALWAYS REMEMBER

- No public or private office (INPS, INAIL, ASL, etc.) sends its employees to your home to collect payments, check bills, or inspect banknotes and jewelry.
- No electricity, gas, or water supplier will ever ask you for information about money or jewelry.
- No delivery personnel delivering parcels, registered mail, or other correspondence will come to your doorstep: delivery will take place at the front door, in the building's entrance hall, or in your mailbox.
- If someone contacts you claiming that your child or relative is in danger (for example, in hospital, involved in an accident, or under arrest) and asks you for money or jewelry to help them, do not trust them: even if the voice sounds familiar, it could be a scammer.
- If strangers show up at your door or ring your intercom claiming to be law enforcement officers, or if they are wearing uniforms and showing ID cards, caps, or badges with official symbols, do not open the door. Check from your balcony or window to see if there is a service vehicle on the street and try to understand the reason for the visit.
- If someone asks to enter your home to check the electrical, gas, or water systems, or to carry out repairs, do not open the door unless you have received official notification from the service provider. Always check that there is a company vehicle outside and, if in doubt, contact the company directly.
- Do not use phone numbers provided by strangers, even if they say they want to prove their identity.

- Never provide personal information to people you don't know. If you realize you have shared it with a scammer, report it immediately to protect your identity.

- **For your online security**

- If you use online banking on your smartphone, always protect your data. I recommend using a separate email account dedicated solely to banking communications, different from your main one.

- When accessing the Internet, always connect through a secure VPN, avoid public Wi-Fi networks, and be careful about which QR codes you scan.

- If you are the victim of a scam, tell your friends and family what happened. This will prevent them from being scammed too.

call the

SINGLE EUROPEAN EMERGENCY NUMBER.



THANKSGIVING

Special thanks to the people who supported me in creating this handbook:

to the Secretary General. Stefania Castricone, and to the Secretariat of the Si.Na.Fi. (National Union of Finance Officers) for free legal aid;

to Christian Diana, Director General of the Anglo American Academy in Cagliari, for free legal aid;

to Antonio Pirro, General Agent of the Generali Agency in Cagliari Porto for free legal aid;

to the artist Francesco Mascia Cogoni and my friend Luca Meloni for the beautiful illustrations created using Microsoft Designer, Gemini, Flow, and ChatGPT;

to Dr. Roberto Borghetti and Dr. Matteo Capaldo of the Trizio Group;

to Dr. Gennaro Fuoco for the time he devoted to me;

To my friend Luca Agati for his constant trust;

to Dr. Alberto Covini for his friendly support;

to Officine Grafiche della Sardegna S.r.l. – (CA) for their sensitivity.

I would like to give special mention and heartfelt recognition to **Striscia la Notizia** and all its contributors and correspondents. Thanks to their tireless commitment and dedication to addressing relevant and topical issues, the program stands out for the fundamental role it plays in monitoring scams, both locally and in the digital world.

The program's segments not only inform the public about the most common pitfalls, but also provide practical advice on how to prevent potential scams. In an age where fraud is taking on new forms and increasingly sophisticated methods, Striscia la Notizia's ability to bring these issues to light is a valuable service to the community.

Through accessible language and incisive reporting, the program guides citizens toward greater awareness and better preparation against scams. It is thanks to these efforts that many can feel safer and more protected, knowing they can count on clear and direct information.

Online Account Security: Protection That Should Never Be Underestimated

Online Account Security: Staying Safe Is Important

Today, we use the Internet for many important things.

With a few simple precautions, you can better protect your accounts.

- Use strong passwords

Your password should be long and hard to guess.

It's important to use different passwords for each service.

For example:

your bank password shouldn't be the same as your email or social media passwords.

- Enable two-factor authentication

Many sites require a code sent to your phone in addition to your password.

This helps protect your account even if someone discovers your password.

- Keep your phone number and recovery email up to date

Your phone number and email address must always be correct and active.

They are needed to recover your account if you lose your password or can no longer log in.

- Keep your emergency codes safe

Some services provide special codes to keep in a safe place.

They can help you regain access to your account in case of problems.

- Use additional security tools

There are apps or small devices that enhance account security.

All these security measures should be checked periodically.

Even an old phone number that is no longer in use can cause problems when recovering your account.

Online security depends on many small precautions that, together, help protect your data and personal information.

FREE LEGAL AID OFFERED BY



© Sergio Cavoli 2025 – “Handbook Against Scams: Together We Are Stronger”

www.infotruffe.com

License: Creative Commons BY-NC-ND 4.0 International

Permitted use: credit the author, do not modify, do not use for commercial purposes.

License link: <https://creativecommons.org/licenses/by-nc-nd/4.0/>