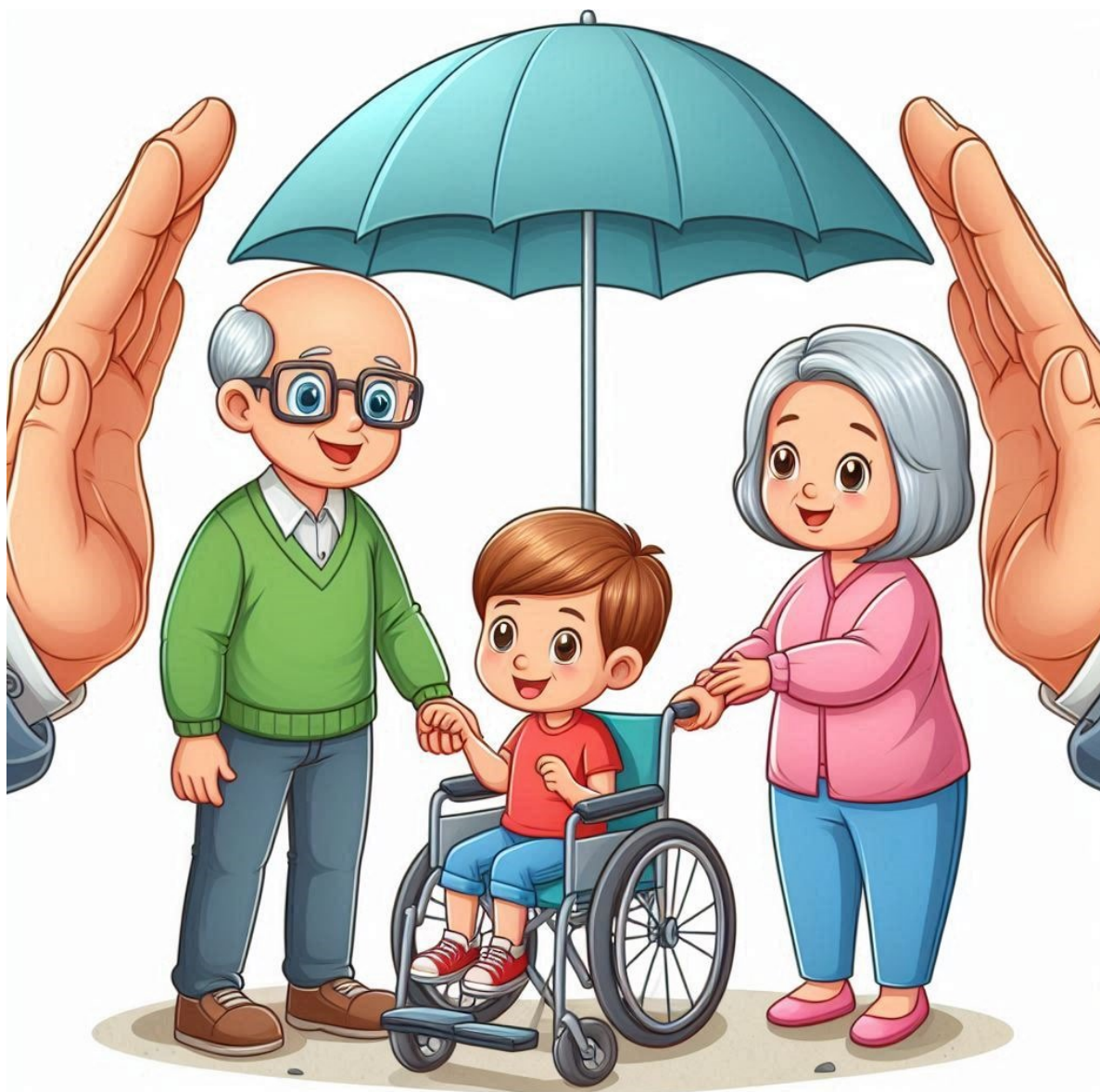


VADEMECUM CONTRA LAS ESTAFAS

JUNTOS SOMOS MÁS FUERTES



ÍNDICE

PREMISA	p. 05
I. LOS DESTINATARIOS	p. 07
II. LOS ESTAFADORES	p. 09
III. EN CASA	p. 11
a. LOS FALSOS AMIGOS	p. 14
b. EL FALSO MENSAJERO	p. 17
c. EL FALSO AGENTE DE SEGURIDAD	p. 19
d. EL FALSO ABOGADO O LAS FUERZAS DEL ORDEN	p. 21
e. CÓMO PROTEGER LA CASA	p. 25
IV. EN LA CALLE	
a. EN EL APARCAMIENTO DEL SUPERMERCADO	p. 31
b. CERCA DEL BANCO O DE LA OFICINA DE CORREOS	p. 33
c. EN EL PARQUE O EN LA CALLE	
• Un empujón de más	p. 35
• La estafa del abrazo	p. 37
• El falso malestar	p. 39
• Magos y santones	p. 41

© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International
Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.
Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

d.	EN EL MERCADO Y ENTRE LOS PUESTOS	
•	El engaño de la bolsa	p. 43
•	El engaño de la chaqueta	p. 45
•	El engaño del falso frutero	p. 47
•	El «sígueme, que está cerrado»	p. 49
•	El círculo	p. 51
•	Dos minutos	p. 53
V.	EN BICICLETA	p. 55
VI.	EN TRANSPORTE PÚBLICO	p. 57
VII.	EN COCHE	
•	Al volante	p. 59
•	En estacionamiento	p. 61
•	La botella de plástico	p. 63
VIII.	EN LOS LOCALES PÚBLICOS	p. 65
IX.	ESTAFAS INFORMÁTICAS	p. 66
•	<i>Man in the middle</i>	p. 69
•	Estafas con el comercio electrónico (trading online)	p. 71
•	<i>Cryptolocker</i>	p. 73
•	<i>Extorsión digital</i>	p. 73
•	Estafa romántica	p. 73
•	Extorsión sexual	p. 77

• <i>La evolución de la triple extorsión</i>	p. 79
• Consejos para la compraventa de objetos en Internet	p. 81
• La falsa herencia	p. 83
• Pagos PAYPAL	p. 83
• Premios / loterías	p. 83
• <i>Phishing</i>	p. 85
• <i>Vishing</i>	p. 87
• <i>Smishing</i>	p. 87
• <i>Pharming</i>	p. 87
• <i>Troyanos (Trojan)</i>	p. 89
• Recaudación de fondos (<i>Fake Crowdfunding</i>)	p. 91
• El engaño con el rostro de un familiar nuestro	p. 93
• Juegos de preguntas y pruebas en línea	p. 95
• Estafa del trabajo falso	p. 99
• El faco CUP	p. 103
• El SPID invisible	p. 105
• El falso Carabinero / Agente de Hacienda / Policía	p. 107
• Ladrones con el terminal de pago	p. 109
• El seguro demasiado barato	p. 111
• La póliza de vida «segura»	p. 113
• Recuerda siempre	p. 115
• Agradecimientos	p. 117
• Seguridad de las cuentas en línea	p. 119

PREMISA

En estas páginas he recopilado situaciones que, lamentablemente, son cada vez más frecuentes y que exponen a las personas mayores y vulnerables a las estafas de delincuentes sin escrúpulos.

Se trata de un fenómeno en constante crecimiento, una verdadera emergencia social que a menudo se subestima o se aborda con demasiada ligereza.

Me llamo Sergio Cavoli y soy jubilado. Desde hace muchos años me dedico concretamente a apoyar a personas frágiles, en particular a aquellas que, como yo, conviven con la esclerosis múltiple.

Desde hace más de un año estoy inmerso en una compleja batalla personal contra un tumor, una experiencia que ha reforzado en mí el valor de la solidaridad, el compartir y la ayuda mutua.

De este camino ha nacido el libro «Passi di Speranza» (Pasos de esperanza), un testimonio de valentía y resiliencia que cuenta cómo, incluso en las pruebas más duras, es posible transformar el sufrimiento en una oportunidad de crecimiento y de servicio a los demás.

Con el mismo espíritu nace ahora el Vademécum contra las estafas a personas mayores y frágiles, una herramienta práctica, clara y de fácil consulta, pensada para tenerla en casa y compartirla con cualquiera que pueda necesitarla.

El Vademécum recoge más de cuarenta ejemplos de intentos de estafa, reales o verosímiles, que afectan cada vez más a personas mayores y vulnerables.

Se divide en tres secciones principales:

Estafas en el hogar, Estafas en la calle y Estafas informáticas, y tiene como objetivo:

- sensibilizar e informar sobre los principales tipos de estafas que existen en la actualidad;
- proporcionar consejos prácticos para reconocer las señales de peligro y reaccionar con rapidez;
- promover una cultura de prevención y seguridad compartida, como herramienta fundamental para la protección personal y colectiva.

Con la información adecuada y algunas medidas sencillas, todos podemos aprender a protegernos a nosotros mismos y a nuestros seres queridos.

Recordemos siempre que **la prevención es nuestra mejor defensa.**

Y si, a pesar de todo, llegamos a ser víctimas de una estafa, no hay que avergonzarse: hablar con alguien de confianza y acudir rápidamente a las fuerzas del orden es el primer paso para reaccionar y protegerse.

Solo a través de la concienciación, la colaboración y el apoyo mutuo podemos proteger realmente a los más vulnerables.

Juntos podemos marcar la diferencia.

Juntos podemos afrontar y superar cualquier obstáculo.

Juntos podemos convertir las dificultades en fortaleza.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS



Proteger a los más vulnerables es responsabilidad de todos.

I. DESTINATARIOS

El preocupante aumento de las estafas, especialmente a personas mayores y vulnerables, ha hecho necesario este manual, diseñado para proporcionar indicaciones prácticas útiles para la prevención.

Las personas más vulnerables, por su edad, salud o condiciones de vida, suelen ser el blanco preferido de estafadores y ladrones. Muchas viven solas, tienen movilidad limitada o padecen enfermedades crónicas y, en ocasiones, guardan dinero u objetos de valor en casa, por desconfianza hacia los bancos o las oficinas de correos. Todos estos factores aumentan el riesgo de ser engañadas o robadas.

Es fundamental recordar que la fragilidad no es solo una cuestión de edad: también tiene que ver con la salud, el aislamiento social y las dificultades emocionales. Las viviendas de estas personas se convierten en objetivos fáciles para quienes se aprovechan de su confianza o descuido, también porque no siempre confían en los demás.

Es posible prevenirlo. En estas páginas encontrará consejos sencillos e inmediatos para reconocer los peligros, evitar comportamientos de riesgo y saber a quién acudir en caso de necesidad.

La seguridad nace de la concienciación y la colaboración.

Las fuerzas policiales —Carabinieri, Policía Estatal, Guardia de Finanzas y Bomberos— garantizan cada día el control del territorio.

En caso de dudas o situaciones sospechosas, siempre llamamos al

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

II. LOS ESTAFADORES

Los estafadores pueden adoptar diversas formas y operar en distintos contextos. Vivimos en una sociedad en la que las apariencias pueden engañar y, lamentablemente, hay personas que se aprovechan de la vulnerabilidad ajena para llevar a cabo estafas y engaños. En este vademécum presentamos algunos de los más comunes:

- Estafadores callejeros: operan físicamente, en la calle o presentándose en tu puerta, simulando situaciones desesperadas para robarte o venderte productos, a menudo falsos, a precios muy bajos.
- Estafadores online: aprovechan Internet para cometer fraudes, como el phishing, en el que intentan obtener información personal fingiendo ser entidades fiables.
- Estafadores telefónicos: utilizan llamadas telefónicas para engañar a las personas, a veces haciéndose pasar por funcionarios de organismos públicos o representantes de empresas.



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

III. EN CASA

NO ABRA LA PUERTA: UNA INVITACIÓN A LA VIGILANCIA

En los últimos años hemos asistido a un preocupante aumento de las estafas perpetradas por individuos que se hacen pasar por miembros de las fuerzas del orden o trabajadores autorizados.

Llevar uniforme o presentarse con una tarjeta de identificación puede parecer una señal de legitimidad, pero no siempre es sinónimo de verdad. Los delincuentes son cada vez más astutos y hábiles a la hora de crear documentos falsos e imitar el aspecto de los agentes o profesionales del sector para ganarse la confianza de las víctimas.

Las excusas para entrar en la casa pueden variar: desde la supuesta necesidad de verificar una filtración de agua hasta peligros más graves, como fugas de gas. Una vez dentro, el resultado es casi siempre el mismo: robo y saqueo.

Los estafadores pueden hacerse pasar por diferentes identidades:

- Funcionarios de correos
- Operadores de organizaciones benéficas
- Representantes de la Seguridad Social, del Ayuntamiento o de las empresas de luz, agua y gas
- Personas que dicen pertenecer a las fuerzas del orden.

Siempre cordiales y bien vestidos, tratan de transmitir una sensación de tranquilidad. Sin embargo, su amabilidad podría ocultar una intención maliciosa.



Antes de abrir la puerta de casa:

1. No abras la puerta inmediatamente: si tienes dudas, siempre es mejor mantener la puerta cerrada y comunicarte a través de la mirilla o una ventana.
2. No confíes inmediatamente: aunque parezcan personas distinguidas y respetables, recuerda que las apariencias a menudo engañan.
3. Comprueba la identidad: si alguien se presenta como agente de las fuerzas del orden, pídele que se identifique. Por norma general, las fuerzas del orden nunca actúan solas y siempre llevan uniforme, casi nunca ropa de civil.
4. Comprueba primero si hay un coche de servicio aparcado en los alrededores.
5. No dude y no tenga miedo de preguntar el motivo de la visita. Los verdaderos agentes están acostumbrados a dar explicaciones claras y detalladas.

Es fundamental recordar que, en caso de duda, siempre es aconsejable ponerse en contacto con las autoridades competentes para verificar la identidad de quien llama a la puerta.

No dude en pedir información y, si es necesario, solicitar la intervención de agentes reales. **LLAME AL 112.**

Las personas mayores y frágiles deben recibir formación para reconocer estos fraudes.

Las familias deben desempeñar un papel activo a la hora de informar a sus seres queridos sobre este tipo de riesgos y las estrategias de prevención.

a. LOS FALSOS AMIGOS

Pueden presentarse en su casa como amigos de un familiar o conocido.

Imagínese que está en casa, envuelto en el aroma del café recién hecho. Es un momento de tranquilidad, un momento de relax que se ha concedido después de un largo día. Pero ese momento de paz puede convertirse fácilmente en otra cosa si, de repente, oye llamar a la puerta. En una época en la que la seguridad parece ser cada vez más precaria, es fundamental prestar atención a quién tenemos delante cuando se trata de abrir la puerta. Imaginemos que se presentan en la puerta «amigos» de familiares o conocidos. «Hola, ¡soy amigo de Marco!», podrían decir. O bien: «Hola, vengo de parte de Francesca». Estas frases, a menudo pronunciadas con una sonrisa tranquilizadora, pueden parecer inofensivas, pero representan riesgos potenciales.

Estos «falsos amigos» saben exactamente cómo tejer una red de confianza en pocos segundos para acceder a vuestros espacios privados y pueden utilizar los nombres de personas de confianza para derribar las barreras de la desconfianza. En estos casos, es esencial permanecer alerta y reflexivo.

Por lo tanto, la primera regla a seguir es no abrir la puerta.

Hay muchas razones por las que esta decisión es fundamental:

1. Seguridad doméstica: su hogar es su refugio y no debe comprometer su seguridad de ninguna manera. Las estadísticas sobre robos y estafas demuestran que muchas de estas situaciones comienzan precisamente con un aparente «giro inesperado» basado en la simplicidad de un saludo amistoso.

2. Identificación: Antes de dejar entrar a alguien en tu casa, es conveniente comprobar su identidad. Pregunta primero: «¿Quién eres? ¿Qué quieres?». También puedes llamar por teléfono al familiar o amigo en cuestión para verificar su identidad.

3. La trampa de la empatía: Las personas tienden a confiar en los desconocidos si estos parecen vulnerables. «Necesito ayuda» o «Por favor, dame solo unos euros» son frases que pueden poner a prueba nuestro corazón. Pero la empatía, si no va acompañada de una evaluación crítica de la situación, puede llevarnos a tomar decisiones precipitadas.

Si se encuentra en una situación similar, debe estar preparado. A continuación le ofrecemos algunos consejos sobre cómo afrontar la situación sin abrir la puerta:

- Si alguien llama a su puerta, no tenga miedo de responder desde dentro. Haga preguntas y escuche atentamente las respuestas. Recuerde: usted tiene derecho a proteger su privacidad y su seguridad.
- Utilice dispositivos de seguridad: hoy en día, muchos de nosotros tenemos cámaras o timbres inteligentes. Estas herramientas no solo le permiten ver quién está en la puerta, sino que también pueden servir como elemento disuasorio para los posibles estafadores.
- No ceda a la presión: si se siente atraído por la historia de otra persona, recuerde mantener la calma. Aunque las palabras parezcan persuasivas, su seguridad vale mucho más. Si, por desgracia, se encuentra en una situación en la que el estafador se ha puesto en contacto con usted, mantenga la lucidez. Nunca facilite dinero ni información personal. Anote cualquier detalle reconocible y **LLAME AL 112**.

Compartir historias y advertencias sobre intentos de estafa puede crear una red de protección colectiva. Si sabe que ha habido otros casos en su zona o que alguien está intentando estafar a sus conocidos, avisar a los demás es un acto de responsabilidad cívica.



b. EL FALSO MENSAJERO

No es raro que un mensajero se presente en su puerta pidiendo el pago de una suma de dinero por la entrega de un paquete. Estas personas afirman que la mercancía ha sido pedida por sus hijos, familiares u otras personas de su edificio.

1. Si recibe un aviso de entrega, asegúrese de que los destinatarios estén realmente al tanto del pedido. Póngase en contacto con ellos antes de proceder.
2. No recoja paquetes inesperados: si no se le ha dado ninguna información previa sobre este paquete, no lo recoja.
3. No realice ningún pago antes de tener la confirmación. Si el mensajero le parece insistente, LLAME AL

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



c. EL FALSO AGENTE DE SEGUROS

En los últimos años, el aumento de los precios de los seguros ha hecho que muchos consumidores sean vulnerables a ofertas engañosas. Por lo tanto, no es raro encontrarse con un supuesto agente de seguros que llama a su puerta o se presenta cerca de un cajero automático dentro de un centro comercial. Con una sonrisa cautivadora y frases persuasivas, estas personas se ofrecen a venderle pólizas de seguro para su familia, su coche o su casa a precios muy competitivos.

La tentación de ahorrar es fuerte y, en un momento de crisis económica, muchos pueden caer en la trampa. Tras una larga conversación y algunas promesas atractivas, llega el momento crucial: el pago. Con cierta prisa, el agente le hace firmar documentos que parecen oficiales y le entrega una hoja de papel, aparentemente una póliza de seguro. Sin embargo, puede descubrir con gran sorpresa que ese documento no tiene ningún valor legal.

La desilusión se convierte rápidamente en preocupación: acaba de gastar dinero en algo completamente inútil. Por lo tanto, es fundamental prestar atención y desconfiar de las ofertas que parecen demasiado buenas para ser verdad. Antes de suscribir cualquier póliza, es aconsejable investigar, comprobar las credenciales del agente y comparar las ofertas auténticas del mercado. La prudencia es la clave para proteger no solo su cartera, sino también su tranquilidad. LLAME al **112**.



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

d. EL FALSO ABOGADO O MIEMBRO DE LAS FUERZAS DEL ORDEN.

È Sin duda, es una situación angustiosa: recibir una llamada de un abogado, un carabinero, un agente de la Guardia de Finanza o un policía, o de la centralita de un hospital, informándote de que tu hijo o tu nieto ha tenido un grave accidente y se encuentra en el hospital, o que ha sido detenido y necesita ayuda económica urgentemente. Estas noticias son devastadoras y pueden provocar inmediatamente miedo y ansiedad. Sin embargo, es fundamental mantener la calma y saber reconocer si se trata de una estafa.

Los estafadores se aprovechan de las emociones fuertes, creando situaciones urgentes y dramáticas para obligarte a reaccionar de forma impulsiva. A menudo, te piden que envíes dinero inmediatamente o que los acompañes al cajero automático para retirar grandes cantidades de dinero. No actúes por instinto: tómate tu tiempo para reflexionar y analizar la situación.

Sin embargo, hay señales de alerta a las que hay que prestar atención:

- 1.** La solicitud urgente de dinero.
- 2.** Ausencia de confirmación: si no te proporcionan ningún detalle verificable sobre el supuesto incidente o problema legal, desconfía.
- 3.** Incertidumbres en los detalles: pueden ser vagos sobre los hechos, el lugar del incidente o la naturaleza de la detención. Llama siempre al

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





¿Qué hacer si recibes una llamada de este tipo?

- No respondas impulsivamente: tómate un momento para pensar y verifica la veracidad de la llamada.
- Ponte en contacto directamente con tu familiar: llama a tu hijo o nieto para confirmar la situación. Si no consigues contactar con ellos, habla con otros familiares o amigos.
- No dejes entrar a nadie: si un supuesto «cómplice» de los estafadores se presenta en tu casa, no abras la puerta. No te dejes convencer para entregar dinero ni los sigas bajo ningún concepto.
- Anima también a otros miembros de la familia y amigos a reconocer estas señales de alerta y a mantener una actitud escéptica ante las solicitudes urgentes de dinero. Estar informado es el primer paso para protegerse y defenderse contra estos fraudes.

Es fundamental permanecer alerta y ser preciso. Recuerde: en caso de duda, ¡verifique siempre!

Si sospecha que es víctima de una estafa, llame al 112. Cualquier información útil puede ayudar a detener a los estafadores.

© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



e. CÓMO PROTEGER LA CASA

Vivir en una vivienda segura es el sueño de todos y, con algunas sencillas precauciones, nuestra casa puede serlo. Los ladrones prefieren las viviendas aisladas, silenciosas y sin barreras.

Puede ser útil:

- La colaboración mutua entre vecinos, para mantenerse en contacto si es necesario y así haber siempre alguien que controle su vivienda durante su ausencia, ya sea breve o prolongada.
- Cerrar siempre la puerta de acceso al edificio.
- esconder las llaves de casa en lugares seguros y bien ocultos.
- no abrir la puerta principal o la puerta de casa si no se está seguro de la identidad de quien llama.
- Instale una puerta blindada con mirilla digital.
- No deje documentos personales en lugares de fácil acceso.
- Instale dispositivos antirrobo y/o de videovigilancia. Active siempre la alarma cada vez que salga de casa y, si es posible, también cuando se vaya a dormir. Hoy en día existen desgravaciones fiscales para este tipo de intervenciones.
- No coloque en el llavero placas con su nombre y dirección que, en caso de pérdida, puedan facilitar la localización del apartamento.
- Ilumine con especial atención la entrada y las zonas oscuras.
- Coloque rejas en las ventanas o cristales irrompibles si vive en un piso bajo o en una casa independiente. Hoy en día existen desgravaciones fiscales para este tipo de intervenciones.





- **Si vive en una casa aislada o, si tiene la posibilidad, considere la posibilidad de adoptar un perro.**

Un perro no solo es un compañero fiel y una fuente de afecto, sino que también se convierte en un valioso aliado para la seguridad del hogar: su presencia y sus ladridos pueden disuadir a los intrusos, mientras que cuidarlo aumenta la vigilancia, la conciencia del entorno y la sensación de protección, independientemente de la planta en la que vivas.



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- Cuando se vaya de **vacaciones, no publique fotos ni información en las redes sociales**. Solo podrá hacerlo cuando regrese. Informe de su ausencia solo a sus seres queridos. Si su viaje o trabajo le mantendrá lejos de casa durante mucho tiempo, siempre es mejor encargar a un familiar o amigo de confianza que realice controles ocasionales.
- Si te vas un fin de semana o estás solo en casa y no tienes sistemas de seguridad, deja una luz o la radio encendidas para que se vea y se oiga desde fuera que la casa está habitada. Hoy en día, los ladrones buscan principalmente dinero, por lo que puede ser útil dejar algunos billetes de alta denominación con una nota que diga: «No hay más dinero en la casa ni joyas, por favor, no causen daños»
- Una vez dentro, los ladrones intentan ir primero al dormitorio y luego pasan a los lugares menos previsibles. Desde los armarios hasta la ropa, la caja del inodoro, los cojines del sofá, el tarro del azúcar, el jarrón, el cuadro..... Explorarán cada rincón.
- Cuando vuelva a casa, si se da cuenta de que la cerradura ha sido forzada, la puerta está entreabierta o la persiana arrancada, no entre en la casa y **llame al 112**.
- Del mismo modo, si al entrar en casa se da cuenta de que le han robado, no toque nada y llame inmediatamente **al 112**.



IV. EN LA CALLE

a. EN EL APARCAMIENTO DEL SUPERMERCADO

- A la salida de los supermercados, a menudo nos encontramos con personas dispuestas a ofrecernos ayuda para empujar el carrito o llevar la bolsa de la compra hasta el coche o a casa. Este gesto de amabilidad parece inofensivo e incluso cortés, pero detrás de este servicio puede esconderse una realidad mucho más inquietante.
- Es fundamental ser cautelosos y conscientes de que, en algunos casos, estas personas pueden tener intenciones maliciosas. Su objetivo no es solo aliviar el peso de nuestras bolsas, sino también recopilar toda la información posible sobre nosotros.
- Podrían ofrecerse a acompañarnos a la oficina de correos, al banco o incluso al cajero automático, para captar detalles cruciales sobre nuestros hábitos diarios, los lugares que frecuentamos y, en algunos casos, información personal sobre nuestras cuentas y ahorros. Una sonrisa y un gesto benévolo pueden ocultar intenciones menos nobles.
- Por lo tanto, es importante estar siempre alerta y proteger nuestros datos personales, ya que la información recopilada podría ser útil para robarnos más adelante.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

b. Cerca del banco o de correos

Si alguien se le acerca, especialmente después de haber retirado dinero en efectivo de un banco o una oficina de correos, ¡tenga cuidado! A menudo, estas personas pueden presentarse como empleados del banco o de correos y alegar, por ejemplo, que deben comprobar los números de serie de sus billetes porque podrían ser falsos.

Recuerde: ningún empleado del banco o de la oficina de correos le detendrá ni acudirá nunca a su domicilio para comprobar los billetes que acaba de recibir. Se trata de una estafa muy conocida. El objetivo del delincuente es sencillo: quedarse con su dinero legítimo, sustituyéndolo por billetes falsos o confiscándolo por completo.

Nunca entregue su dinero: si alguien le pide que lo haga, mantenga la calma y no ceda. Si todavía está en la calle, llame la atención de los transeúntes y **LLAME AL 112**.

© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



a. EN UN PARQUE o EN LA CALLE

- **Un empujón de más.**

Imagina que estás tomando un café o un refresco, observando, por ejemplo, a un grupo de niños que juegan. Se te acerca casualmente una persona con un cochecito o una mujer que está haciendo footing y, con un gesto distraído, golpea tu vaso, derramando el líquido sobre ti. «¡Lo siento mucho!», exclama, mientras se apresura a ofrecerte ayuda con una mirada atenta.

Pero aquí está el truco: mientras se agacha para limpiar el desastre que ha creado, su mano se mueve rápidamente hacia tu mochila o bolso.

En cuestión de segundos, consigue robarte la cartera, el móvil o incluso las llaves de casa, y se marcha con la excusa de que se le ha caído algo.

Este truco no solo lo pueden llevar a cabo mujeres con niños, sino también hombres que se aprovechan de la situación.

Imagina a un chico que, con una sonrisa afable, se acerca para pedirte información. Quizás se trate de un truco bien pensado: mientras te distrae con la conversación, uno de sus cómplices merodea cerca de tu bolso, listo para aprovechar el momento. Lo alarmante es que estas tácticas de robo se producen con demasiada rapidez, mientras que las víctimas, inconscientes y confiadas, creen que se encuentran ante personas bienintencionadas. Compartir momentos familiares y el ambiente amistoso pueden dificultar la percepción del peligro inminente. Por lo tanto, es fundamental permanecer alerta incluso en los lugares más inocuos. Es importante proteger tus pertenencias y tu seguridad sin dejar espacio a los aprovechados.

Nunca está de más ser cauteloso. Incluso en momentos de aparente normalidad pueden esconderse peligros que te pillen desprevenido.

La concienciación es la mejor defensa contra estos delincuentes. Si, por desgracia, has sido víctima de uno de estos fraudes, llama inmediatamente al **112**.



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

- **La estafa del abrazo**

El engaño de la ilusión: las mujeres jóvenes y la trampa de las estafas. En los últimos años se ha observado un fenómeno cada vez más preocupante que afecta a mujeres jóvenes y hombres mayores. Estas interacciones, que en apariencia parecen inofensivas o incluso halagadoras, a menudo esconden intenciones maliciosas. Las mujeres jóvenes, con su actitud amable y encantadora, se acercan a hombres más maduros creando la ilusión de una conexión emocional o seductora. Esta dinámica puede considerarse una forma de engaño que se aprovecha de la vulnerabilidad de las personas mayores.

La interacción comienza con cumplidos y un comportamiento afectuoso. Las mujeres suelen utilizar frases dulces y gestos amistosos, haciendo que sus víctimas se sientan especiales e importantes. Este enfoque puede engañar a las personas mayores, haciéndoles creer que existe un interés romántico o sexual real. Cuando la persona mayor, tal vez con la esperanza de iniciar un juego de seducción, rechaza las insinuaciones, la situación da un giro inesperado. En ese momento, estas mujeres no tienen escrúpulos: siguen mostrando afecto, acercándose para dar un abrazo que podría parecer inofensivo. Sin embargo, justo en ese momento, se produce el verdadero giro inesperado: sus manos hábiles y rápidas se mueven sigilosamente para llevarse carteras, teléfonos móviles o relojes. La víctima, tomada por sorpresa, se encuentra desconcertada, confundida y, a menudo, impotente ante un acto tan solapado. Este tipo de fraude no solo tiene consecuencias materiales para la persona mayor robada, sino que también deja profundas huellas a nivel emocional. Se rompe la confianza y desaparece la sensación de seguridad, dejando espacio a una desconfianza que puede influir negativamente en las interacciones futuras. Por lo tanto, es fundamental sensibilizar sobre este tema y animar a las personas, especialmente a las más vulnerables, a mantener una actitud crítica y cautelosa hacia los nuevos conocidos. Si eres víctima de este tipo de estafa, no lo dudes: **LLAMA AL112**.



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- **El falso malestar**

En las concurridas calles de la ciudad, es posible que te encuentres con situaciones que, a primera vista, parecen requerir tu intervención. A veces, una persona puede simular un malestar y tirarse al suelo con aire desesperado, como si necesitara ayuda. El instinto nos empuja a acercarnos, a intentar comprender cómo podemos ayudar a quien parece estar en dificultades. Sin embargo, es fundamental permanecer alerta y consciente.

En estas situaciones, la realidad puede ser muy diferente. El malestar podría ser solo una farsa, un hábil engaño orquestado por personas malintencionadas. Mientras te acercas para prestar ayuda, un cómplice, camuflado entre la multitud, podría atacarte. En un momento de distracción, te encuentras pidiendo ayuda, mirando una ambulancia que no llega, mientras el ladrón agachado a tu lado te arrebató el bolso o la cartera y desaparece en el caos circundante. Este tipo de estafa, por desgracia, es más común de lo que se piensa. No es solo una cuestión de falta de empatía o bondad; es importante preservar no solo nuestro bienestar, sino también el de los demás.

Entonces, ¿qué hacer en estas situaciones?

- Observa atentamente. Si ves a alguien que parece estar en dificultades, evalúa la situación con calma. Observa atentamente.
- No te acerques inmediatamente; intenta averiguar si hay otras personas alrededor, si la persona ya está recibiendo ayuda de alguien más.

- **Llama al 112**

Recuerda que tu gesto de altruismo es loable, pero la prudencia siempre debe guiar tus acciones. Nunca subestimes la posibilidad de un engaño. Ser atento y cauteloso puede protegerte de sorpresas desagradables y garantizar que tu ayuda llegue realmente donde se necesita.



- **Magos y gurús**

Aún hoy, a pesar de que vivimos en una sociedad moderna y evolucionada, es sorprendente lo extendido que está el fenómeno de los magos y los gurús. Estas figuras, a menudo dotadas de carisma y capacidad de persuasión, logran captar la atención de personas vulnerables, aprovechándose de su desesperación. Quienes se enfrentan a graves problemas de salud o dificultades laborales pueden verse tentados a buscar soluciones alternativas, a menudo ilusorias.

Muchos de estos «profesores» de lo oculto ofrecen promesas milagrosas: curaciones rápidas de enfermedades incurables, resolución de problemas económicos o incluso suerte en el amor. Sin embargo, detrás de estas afirmaciones se esconde una realidad mucho más amarga: la manipulación de las emociones humanas para obtener beneficios. Las personas, en particular los ancianos, en su búsqueda de ayuda, son víctimas de estos fraudes y llegan a gastar sumas considerables en rituales y prácticas que no tienen ningún fundamento científico.

En Italia está prohibido ejercer de mago. La ley castiga el ejercicio de la pseudociencia, reconociendo el derecho de los ciudadanos a recibir tratamientos y apoyo válidos y basados en pruebas concretas. Es fundamental recordar que, para cualquier problema, siempre es aconsejable acudir a profesionales cualificados: médicos, psicólogos y especialistas. Solo confiando en estas figuras se pueden obtener diagnósticos precisos y tratamientos adecuados, evitando caer en las trampas de quienes se aprovechan de la fragilidad ajena.

No lo dude, LLAME **112**.



- **El engaño del bolso.**

Entre los puestos, puede que te llame la atención una pequeña exposición de bolsos artesanales. En cuanto te acercas, el dependiente te invita a probar uno. Mientras el vendedor finge estar distraído, te das cuenta de que dentro hay, por ejemplo, una cartera llena de billetes. Sin dudarlo, compras el bolso, tratando de no llamar la atención del dependiente. En cuanto te alejas del puesto, la curiosidad por descubrir ese tesoro es demasiado grande, ¡pero descubres que lo que parecían billetes son trozos de papel! Llama

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





- **El engaño de la chaqueta.**

Tu mirada se posa en un puesto que expone chaquetas. Intrigado, te acercas y el vendedor te invita a probarte una. Mientras te la pones, notas un objeto en el bolsillo y encuentras, por ejemplo, un reloj brillante. «¡Un Rolex! ¡Increíble!», piensas. Compras la chaqueta sin pensarlo dos veces. Hay algo emocionante en la idea de poseer una prenda de vestir que viene acompañada de un reloj de valor. Unos instantes después, mientras te alejas con la nueva chaqueta, abres el bolsillo.

Esa ganga que parecía tan ventajosa resulta ser una ilusión: el reloj era una falsificación bien hecha, pero seguía siendo una falsificación.

¿Y la chaqueta? No valía ni la mitad del precio que pagaste.

Ambas experiencias nos enseñan una valiosa lección. La tentación de una ganga imperdible puede hacernos perder la lucidez. Es fácil dejarse llevar por la emoción del momento, pero es fundamental permanecer alerta y ser cauteloso.

Los puestos callejeros pueden ofrecer tesoros inesperados, pero también engaños disfrazados de oportunidades. El mundo está lleno de estafadores dispuestos a aprovecharse de la ingenuidad de las personas.

Llama siempre al 112.



- **El engaño del falso frutero**

En las inmediaciones de los mercados o en los parques de la ciudad es fácil encontrarse con una escena que despierta simpatía y compasión: un hombre, con expresión triste y ojos llorosos, se te acerca. Su voz temblorosa cuenta una historia desgarradora: ha perdido su trabajo para quedarse al lado de su esposa enferma o de su hijo en estado grave. Te habla de los gastos médicos insostenibles, de la desesperada necesidad de ayuda y de cómo ha decidido vender fruta o verdura para intentar hacer frente a las emergencias.

La imagen de una familia en dificultades te llega al alma. Te ofrece la mercancía, presentándola como fresca y de excelente calidad. Sin pensarlo demasiado, decides ayudarlo, pagando una cantidad muy superior al valor real de esos productos. Le ves cargar la fruta o la verdura en el maletero de tu coche, con una expresión de gratitud que parece sincera.

Pero cuando llegas a casa te das cuenta de que esa fruta y verdura, aunque parecen bonitas y frescas, en realidad son productos de mala calidad. Se puede llamar al 112 porque no es solo una cuestión de fraude, sino un paso necesario para detener a quienes se aprovechan de la buena fe de las personas.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





- El «sígueme, que está cerrado»

Te encuentras en una estación abarrotada, el murmullo de la gente llena el aire, los trenes llegan y salen sin cesar, las voces se entremezclan, algunos se detienen, otros corren, y tú solo tienes un objetivo en mente: llegar a una salida en medio de ese flujo continuo.

En un momento dado, una persona se te acerca con naturalidad, como si fuera normal hablar contigo allí, en medio de todo ese bullicio, y te dice que por un lado está todo cerrado, que no tiene sentido seguir así y que es mejor pasar por el otro lado, más rápido, más sencillo, y lo dice con una seguridad tranquila, sin vacilar. Y sin que haya realmente un momento en el que te lo preguntes, te encuentras siguiéndole.

Al principio no cambia nada, la estación sigue siendo la misma, los ruidos familiares, el ajetreo a tu alrededor, todo parece normal, pero mientras caminas algo empieza a cambiar lentamente, la multitud se va dispersando sin que te des cuenta, los sonidos se atenúan, los pasillos se estrechan y el recorrido cambia sin una señal precisa.

Entonces llega esa sensación difícil de explicar, como si los puntos de referencia que tenías antes ya no fueran los mismos, como si estuvieras avanzando pero sin reconocer del todo la dirección, y sigues caminando de todos modos porque ya estás en ese trayecto y dar marcha atrás ya no es tan sencillo como parecía al principio.

Y cuanto más avanzas, más cambia todo, hasta el punto de que el lugar en el que te encuentras ya no se parece en nada al lugar del que partiste, aunque nunca haya habido un momento concreto en el que puedas decir que algo haya cambiado. Y es precisamente ahí donde todo puede detenerse.

Detente un momento, sin prisas, como si simplemente estuvieras recuperando el aliento, mira a tu alrededor y toma conciencia de lo que te rodea, y si algo no te convence o ya no te parece claro, no sigas por inercia: despídete con naturalidad, da las gracias y vuelve a un lugar que conozcas.

Si te sientes inseguro o incómodo, no te quedes solo con esa sensación. Acércate a otras personas, quédate en zonas más concurridas o pide ayuda a quien esté cerca, porque la presencia de los demás cambia de inmediato la percepción de lo que estás viviendo.

Y si algo no cuadra, aunque sea solo por un instante, ya es momento de detenerse y, en caso de duda, llamar al 112.



- El círculo

Estás en una parada, en un parque o haciendo cola en algún sitio, en uno de esos momentos en los que simplemente estás esperando y la gente a tu alrededor sigue moviéndose sin que tú le prestes demasiada atención.

A veces alguien se te acerca con un teléfono o unos auriculares y te dice «te voy a hacer escuchar algo», otras veces es una simple pregunta, una información, algo que parece inofensivo y normal, y en ambos casos te detienes sin pensarlo demasiado, porque es una situación que parece parte de la vida cotidiana.

Y es precisamente mientras estás ahí, con la atención puesta en esa persona, cuando la escena cambia sin una transición evidente.

Llegan otras personas, cuatro o cinco, casi sin hacer ruido, y en pocos segundos se acercan demasiado, creando un espacio cerrado a tu alrededor mientras todo ocurre de forma rápida y coordinada: las manos se mueven velozmente, se abren bolsos, se registran bolsillos, mientras tu atención sigue centrada en ese instante inicial.

Cuando intentas reaccionar y te das cuenta de que algo no cuadra, el grupo ya se ha disuelto, cada uno se aleja en una dirección diferente, mezclándose entre la gente como si nada hubiera pasado.

Y es precisamente ahí donde todo se decide en unos pocos segundos.

No te quedes parado intentando entender de inmediato lo que ha pasado: crea distancia, aléjate con decisión del lugar del primer contacto y dirígete a un espacio más abierto y concurrido.

Si alguien sigue intentando hablar contigo o retenerte, no te detengas a discutir: una respuesta breve, mientras sigues moviéndote, como «lo siento, tengo que irme», es más que suficiente.

Busca inmediatamente un lugar seguro, una persona reconocible, una tienda, un grupo de personas, algo que te devuelva a un contexto claro y controlable, y solo después, con calma, comprueba qué ha pasado.

Comparte lo sucedido con familiares y conocidos, porque reconocer estos patrones ayuda a evitarlos.

Y si algo no cuadra, no esperes: llama al 112.



- Dos minutos

Estás en una calle, en una estación o en una plaza, inmerso en el continuo ir y venir de la gente, cuando alguien pasa a tu lado, deja cerca de ti una mochila o un paquete y te dice con total naturalidad «¿me lo guardas un momento?», como si fuera lo más normal del mundo, y sin darte tiempo a responder ya se aleja entre la multitud.

Te quedas ahí con ese objeto a tu lado, en una situación que se ha creado en unos instantes mientras todo sigue moviéndose a tu alrededor.

Poco después llega otra persona, la mirada se posa primero en el objeto y luego en ti, y comienzan las preguntas sencillas pero insistentes: si es tuyo, qué contiene, por qué está ahí, como si de alguna manera ya estuvieras dentro de una situación que está tomando forma.

Y mientras intentas responder, toda la atención se concentra en ese punto, mientras el resto a tu alrededor sigue fluyendo pero pierde importancia, se convierte en fondo.

Y es precisamente ahí donde todo se decide en unos segundos.

Lo importante es no dejarte involucrar: da inmediatamente un paso atrás, aléjate con calma, deja el objeto donde está y dirígete hacia un espacio más abierto o hacia otras personas, donde la situación se rompe y todo vuelve a estar más claro.

Si alguien insiste o intenta retenerte, no te detengas a dar explicaciones: una frase breve, sin reducir el paso, como «no es mío, no sé nada», y sigue alejándote.

Y si tienes la más mínima duda o te sientes en apuros, no dudes en llamar al 112.



V. EN BICICLETA

Cuando se decide desplazarse en bicicleta, es fundamental prestar atención no solo a la seguridad personal, sino también a la de los bienes propios. Un error común que cometen muchos ciclistas es guardar bolsos o riñoneras en la cesta delantera de la bicicleta. Aunque pueda parecer una solución cómoda y práctica, hay varias razones por las que es recomendable evitar este hábito.

En primer lugar, la cesta es un lugar de fácil acceso tanto para el ciclista como para los posibles ladrones. Dejar objetos de valor a la vista aumenta considerablemente el riesgo de robo. Aunque solo te alejes un momento, un ladrón experto podría aprovechar para sacar rápidamente el bolso o la riñonera sin que te des cuenta.

En segundo lugar, colocar objetos pesados o voluminosos en la cesta puede comprometer el equilibrio. Llevar una carga desequilibrada puede dificultar la maniobrabilidad de la bicicleta, lo que aumenta el riesgo de caídas o accidentes. La seguridad al montar en bicicleta siempre debe ser la prioridad.

Por último, otro aspecto a tener en cuenta es la protección de tus pertenencias. Una cesta abierta no ofrece ninguna protección contra las inclemencias del tiempo. Si llueve o hace viento, tus efectos personales podrían dañarse.

La solución ideal es, por lo tanto, utilizar una bolsa para bicicleta especialmente diseñada, que se puede montar en el cuadro o en la espalda.

En resumen, cuando se viaja en bicicleta, es mejor evitar guardar bolsas o riñoneras en la cesta. Opta por alternativas más seguras y mantén tus pertenencias protegidas, para que puedas disfrutar de tu paseo con total tranquilidad.

VIAGGIA SICURO, PROTEGGI I TUOI EFFETTI PERSONALI!

Piccole attenzioni possono
fare una grande differenza.
La tua sicurezza è nelle tue mani.



LA TUA SICUREZZA
È NELLE TUE MANI.

**PREVIENI, PROTEGGI,
VIAGGIA SERENO.**



CON UN PO' DI ATTENZIONE, PUOI GODERTI IL VIAGGIO IN TUTTA SICUREZZA!



**ATTENTO AI
PICKPOCKET!**

VI. EN EL TRANSPORTE PÚBLICO

Cuando se viaja en autobús o metro, la seguridad de los efectos personales se convierte en una prioridad fundamental. El transporte público, aunque es una forma eficaz de desplazarse por la ciudad, también puede ser un terreno fértil para los robos y las distracciones.

Por eso es esencial adoptar algunas medidas preventivas:

- Lleve la cartera en el bolsillo delantero de los pantalones, ya que esta ubicación reduce considerablemente el riesgo de robo y le permite tener siempre la situación bajo control, evitando tener que rebuscar en bolsos o mochilas cada vez que tenga que pagar un billete o mostrar un documento.
- Lleve el bolso delante, sobre el pecho. Llevar el bolso al hombro o en una posición central no solo dificulta que un ladrón se acerque sigilosamente, sino que también permite tener una mayor visibilidad de lo que sucede a nuestro alrededor. En una multitud, es mejor estar atento a cualquier movimiento sospechoso y, al mismo tiempo, proteger sus pertenencias de manera más eficaz.
- Elegir bolsos con cremalleras seguras y varios bolsillos puede ayudar a organizar mejor los objetos personales, lo que dificulta que los delincuentes accedan a todo de una sola vez;
- Utilizar materiales resistentes y colores menos llamativos también puede contribuir a mantener un perfil bajo, evitando llamar la atención sobre los objetos de valor;
- Mantener siempre cierta vigilancia y prestar atención al entorno. Ser consciente de tu espacio y de las personas que te rodean puede marcar la diferencia entre un viaje tranquilo y una experiencia estresante. Con un poco de atención y precaución, es posible disfrutar de las ventajas del transporte público sin correr riesgos.



VII. EN COCHE

- **Al volante.**

En el coche es fundamental tomar algunas precauciones para garantizar tu seguridad y la de tus pertenencias. Un aspecto que a menudo se subestima es el de no dejar nunca bolsos o riñoneras en el asiento del copiloto, sobre todo con la ventanilla abierta. Esta situación es una invitación para los ladrones, ya que facilita un posible robo.

En un semáforo o en un atasco, es posible que su atención se centre en otra cosa y, si alguien se acerca a su coche, con un gesto rápido y discreto, le robará el bolso sin que se dé cuenta. Por desgracia, esta situación es más habitual de lo que se piensa.

Para evitar estas situaciones, acostumbrémonos a mantener la ventanilla subida y la puerta siempre cerrada y bloqueada con el seguro, especialmente cuando nos encontremos en zonas concurridas o poco recomendables. No solo protegeremos nuestros efectos personales, sino que también nos sentiremos más seguros dentro del vehículo.

Este hábito puede marcar una gran diferencia en la prevención de robos en el coche.

Si, mientras conduce, choca contra otro vehículo o un peatón y el conductor se baja mostrando daños en la carrocería de su coche, o el peatón se queja de haber sido golpeado en la pierna, es posible que le pidan una indemnización amistosa con una pequeña suma de dinero en efectivo. En estos casos, lo más sensato es permanecer dentro de su coche y **llamar inmediatamente al 112** para informar del suceso, proporcionando detalles útiles sobre el lugar y la identidad de las personas implicadas. Para protegerse en situaciones como esta, podría considerar la posibilidad de comprar una cámara para salpicadero (dash cam).

Hoy en día están disponibles a precios asequibles y pueden grabar todo lo que ocurre mientras conduce.

Estas cámaras pueden proporcionar pruebas valiosas en caso de accidentes o intentos de fraude, garantizándole tranquilidad y seguridad en la carretera.

- **Aparcado.**

Si estás sentado en el coche esperando a alguien, cierra siempre las puertas con el seguro y, si alguien se acerca para pedirte información, no bajes nunca la ventanilla y espera a que esa persona se aleje. Podría ser un posible delincuente. La seguridad personal siempre debe anteponerse a cualquier interacción casual: en el mundo actual, la prudencia debe formar parte integrante de nuestra vida cotidiana.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





El engaño de la botella de plástico atascada en los coches.

Los ladrones, apuntando a un vehículo específico, colocan una botella de plástico vacía en el neumático delantero del coche. Esta maniobra es particularmente astuta, ya que el conductor rara vez se da cuenta de la presencia del cuerpo extraño atascado en la rueda. Cuando el conductor arranca el motor, el ruido producido por la botella aplastada llama su atención. El conductor, preocupado, sale del coche para ver qué está pasando. Es en ese momento cuando los ladrones entran en acción: aprovechando la situación, a menudo con el motor en marcha y las llaves puestas, se llevan el vehículo en cuestión de segundos, dejando al legítimo propietario incrédulo e impotente. El éxito de esta estafa se suma a otras técnicas fraudulentas, como la estafa de la pegatina o la de la rueda pinchada, todas ellas características de una época en la que la falta de atención puede salir muy cara. Es fundamental, incluso cuando tenemos prisa, prestar especial atención a nuestro coche antes de ponernos al volante, centrándonos en los neumáticos y comprobando cualquier detalle sospechoso. Un pequeño detalle, aunque no sea aparente, podría ser una señal de peligro. Incluso un carrito de la compra vacío detrás de nuestro coche debe alarmarnos, al igual que un billete, normalmente de 10 o 20 €, colocado en el parabrisas. En cualquier caso, la única precaución que hay que tomar es no salir del coche, sino alejarse rápidamente. Si esto no es posible, es importante asegurarse de que todas las puertas estén bien cerradas y llamar inmediatamente al 112, tocar el claxon para llamar la atención de los transeúntes u otros conductores.

Recordar estos sencillos pasos puede marcar una gran diferencia. La prevención es esencial para combatir este tipo de delitos. En un contexto en el que los robos de coches están aumentando, la información y la concienciación pueden ser los principales aliados para evitar ser víctimas de estafas ingeniosas como las descritas anteriormente.



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

VIII. EN LOS LOCALES PÚBLICOS

Cuando se va a comer a un local, es fundamental prestar atención no solo a la comida, sino también a la seguridad de los objetos personales. A continuación, se ofrecen algunos consejos prácticos para evitar robos o pérdidas que puedan arruinar la velada:

- 1. No deje el bolso sin vigilancia.** Es habitual colocar el bolso en el reposabrazos de la silla, pensando que allí estará seguro. Sin embargo, esta práctica puede exponer tus pertenencias al robo. Es preferible mantener el bolso siempre a salvo, tal vez colocándolo entre las piernas o utilizando un gancho específico para bolsos, si está disponible en la mesa y, en cualquier caso, se puede comprar por 5 €.
- 2. Cuidado con la chaqueta:** otro error frecuente que cometemos es dejar la chaqueta en el respaldo de la silla, con objetos de valor como la cartera. Nada más fácil para un malintencionado que coger la chaqueta y huir o rebuscar en su interior. Si necesitas quitarte la chaqueta, considera colgarla en un perchero o mantenerla sobre tus piernas.
- 3. Cuidado con el smartphone:** nunca sobre la mesa. El smartphone es uno de los objetos más codiciados por los ladrones. Hoy en día es la llave de acceso a nuestra vida, y no todo el mundo es capaz de bloquearlo y dejarlo inutilizable. Dejarlo sobre la mesa puede parecer cómodo, pero ofrece una oportunidad perfecta para cualquiera que quiera robarlo. Es mejor guardarlo en el bolsillo de la chaqueta o del pantalón.

¡No pierdas de vista tus pertenencias y disfruta de la velada con total tranquilidad!



IX. ESTAFAS INFORMÁTICAS

Hoy en día, con Internet, el delincuente ya no tiene rostro y... nunca duerme.

Basta con un clic sin darse cuenta para que entre en nuestras casas y en nuestras vidas.

Los peligros en línea pueden presentarse de muchas formas y con diferentes niveles de riesgo.

No tengas miedo ni vergüenza. **Si tienes alguna duda o te sientes en apuros, pide ayuda y llama al 112."**

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



- ***Man In The Middle (Hombre en medio)***

Un primer ejemplo de esta actividad ilícita se denomina «man in the middle» (hombre en medio), cuyo objetivo principal es robar nuestra información. Se trata de un tipo de ataque dirigido a routers o servidores en el que una tercera persona, el delincuente, intercepta y altera la comunicación entre dos partes que creen estar comunicándose entre sí. Por ejemplo, se interpone entre la víctima y el servidor (como es el caso, por ejemplo, de un servidor de un banco online o de correo electrónico). Son ataques eficaces y difíciles de detectar.

Como primera defensa, evita utilizar redes wifi gratuitas, especialmente si piensas realizar transacciones sensibles. Sería mejor utilizar un complemento para el navegador capaz de establecer conexiones seguras.

No visites sitios web cuando el navegador te avise de un problema en su certificado de seguridad.

Si la página web que estás visitando ha comenzado a descargar archivos automáticamente, sin tu permiso, es casi seguro que este sitio está comprometido.

Actualiza siempre el antivirus, da preferencia a aquellos que tienen un sistema interno de control de páginas web que informa al usuario cuando está a punto de entrar en un sitio peligroso.

Por último, sería preferible tener un ordenador específico solo para las transacciones



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

- **Estafas con el trading online.**

En este mundo tampoco faltan las estafas, desconfíe siempre de quienes prometen ganancias fáciles. Invertir en bolsa puede resultar tentador y nos gustaría rentabilizar nuestros ahorros con el trading online.

El TOL (trading online) se puede realizar cómodamente desde casa y desde el ordenador y consiste en comprar y vender títulos financieros a distancia. Es una actividad arriesgada porque se gana con la diferencia de precio entre la compra y la venta de acciones y bonos. No se puede operar directamente en los mercados financieros. Es necesario recurrir a un corredor financiero, es decir, un intermediario que compra y vende valores por cuenta del cliente. El estafador se pone en contacto con la víctima desprevenida, la mayoría de las veces a través de un falso centro de atención telefónica con el pretexto de ofrecer soluciones de inversión fáciles y con grandes beneficios. Aunque dudemos, podríamos dejarnos tentar y confiar pequeñas cantidades de dinero que se nos devolverán rápidamente con las primeras ganancias. En ese momento, los delincuentes pedirán una suma mayor con la falsa promesa de un rendimiento asegurado y, una vez recibida la cantidad solicitada, el falso operador bursátil desaparecerá, de modo que la víctima no podrá recuperar lo que aparentemente ha invertido.

Para operar y evitar estafas, la CONSOB ha puesto a disposición de los usuarios una plataforma de corredores autorizados para ejercer la profesión.

Si tienes dudas, ponte en contacto con la CONSOB en el número 06.8477611 (de lunes a viernes, de 9:00 a 13:00 y de 14:30 a 16:30) y denuncia.



- ***Cryptolocker:***

Es un virus «troyan» que apareció por primera vez en 2013 y se perfeccionó en 2017. Este malware es una forma de «RANSOWARE» que infecta los sistemas Windows y consiste en cifrar los datos de la víctima, exigiendo un pago, un rescate, para descifrarlos. Hasta la fecha, alrededor del 3 % de las personas afectadas por este malware deciden pagar. Algunas víctimas informan de que, a pesar de haber pagado el rescate, no han visto descifrados sus archivos. ¡No paguen, denuncien!!

- ***Extorsión Digital:***

Este término se refiere a la actividad llevada a cabo por delincuentes informáticos con el fin de extorsionar a un particular o a una empresa a cambio de no difundir datos procedentes de correos electrónicos, sitios pornográficos visitados u otro material comprometedor (obtenido mediante un ransomware) que podría dañar la imagen de una persona y sus relaciones sociales. Cualquiera puede ser víctima de un ataque de extorsión digital, desde ciudadanos particulares hasta famosos, políticos y empresas. No abras correos electrónicos sospechosos ni descargues archivos desconocidos.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





- **Estafa romántica:**

El estafador elige cuidadosamente a sus víctimas en las distintas redes sociales (Facebook, Instagram, Telegram, etc.), crea perfiles falsos en sitios web y aplicaciones de citas, inventa una historia verosímil y publica mucho para que su perfil parezca real (las imágenes y fotos del perfil falso se toman de Internet). El estafador no busca sexo, las conversaciones son siempre amistosas, establece una relación contigo para crear confianza y dependencia emocional, de modo que le resulte más fácil pedirte dinero para dificultades económicas repentinas o para comprar el billete para ir a verte. Esta estratagema funciona porque aprovecha la necesidad de sentirse amado y valorado. Lamentablemente, este tipo de estafa ha ido en aumento en los últimos años, pero es necesario denunciarla y avisar a la red social o la aplicación en la que has conocido al estafador

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





- ***Extorsión Sexual:***

La extorsión sexual es un delito grave que se produce cuando alguien amenaza con difundir material privado y sensible si no se le proporcionan imágenes de naturaleza sexual, favores sexuales o dinero.

Los delincuentes en línea pueden ganarse tu confianza fingiendo ser alguien que no son. También se esconden en salas de chat y graban a quienes publican o transmiten en streaming imágenes y vídeos sexualmente explícitos de sí mismos, o pueden piratear tus dispositivos electrónicos mediante malware para acceder a tus archivos y controlar tu cámara web y tu micrófono sin que te des cuenta.

- Nunca envíes imágenes comprometedoras de ti mismo a nadie, sin importar quién sea o quién diga ser.
- No abras archivos adjuntos de personas que no conozcas.
- Apaga tus dispositivos electrónicos y cámaras web cuando no los utilices.
- Si te chantajea, no pagues; interrumpe todo contacto y denúncialo inmediatamente.

Ayúdanos a encontrar a estos delincuentes y a impedir que arruinen la vida de las personas.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS





- ***La Evolución De La Triple Extorsión***

Es la última evolución de la anterior: los delincuentes cifran los datos y los extraen amenazando con filtrarlos si no se satisfacen las demandas de rescate. Si una víctima se niega a pagar, los datos robados pueden subastarse en foros de ciberdelincuencia. Esto ofrece a los delincuentes otra vía para monetizar sus acciones ilegales. Pero han ido aún más lejos con los esquemas de triple extorsión. En algunos casos, cifran y roban datos, amenazan a los empleados de una empresa, se ponen en contacto con familiares y responsables de la empresa y sobrecargan los sitios web de tráfico (también conocido como ataques DDoS o denegación de servicio distribuida) para obligar al pago. A veces, en el mensaje de amenaza recibido se oculta un **troyano**.

© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



- **Consejos para la compraventa de objetos en sitios web:**

Para las fuerzas policiales es imposible supervisar todos los sitios web que realizan comercio electrónico, además de la difusión masiva de aplicaciones de compraventa que ofrecen productos a precios ventajosos. Por eso los estafadores encuentran un terreno fértil y pueden aprovecharse fácilmente para engañar a los compradores ofreciéndoles productos inexistentes o falsificados.

Además de este fenómeno, la víctima del fraude es la persona que pone a la venta su bien. El estafador se pone en contacto con ella fingiendo ser un comprador potencial, casi siempre residente en otras ciudades o fuera de las fronteras italianas: en realidad, estas personas quieren apropiarse de los datos personales para luego cometer otros fraudes.

- Desconfíe de quienes ofrecen un producto a un precio demasiado barato.
- Desconfíe si el comprador se encuentra en el extranjero.
- Compruebe que aparece el candado de transacciones seguras en la parte superior derecha de la página web y utilice siempre un método de pago seguro (NO Western Union, tarjetas regalo, recargas...).
- No introduzcas información personal para canjear un vale o desbloquear un supuesto descuento.
- No descargues ningún software para completar la compra.
- Nunca adelantes dinero por operaciones aduaneras sospechosas, gastos y comisiones.
- Comprueba que la empresa dispone de los datos necesarios (número de IVA, domicilio social).

Desconfíe siempre si el coste del producto que desea comprar es significativamente inferior al que se ofrece en los sitios web oficiales.



- **La Falsa Herencia:**

¿Quién no ha deseado alguna vez tener un pariente rico desconocido que nos dejara una cuantiosa herencia? Cuidado, es posible que un abogado o notario se ponga en contacto con usted porque es el destinatario de una importante herencia, pero para poder disponer de ella deberá entregar una determinada cantidad de dinero a una persona designada por el notario.

El programa Striscia la notizia ha documentado varios casos similares en toda Europa.

Nunca adelantes dinero cuando seas tú quien debe recibirlo. Ninguna solicitud de este tipo es legítima, por lo que siempre debes denunciar lo sucedido.

- **Pago con PAYPAL:**

¿Utilizas PayPal para tus compras? Bien, pero si realizas el pago con una descripción que no sea pertinente para la operación, del tipo «enviar pago/enviar regalo a amigos y familiares», y tu compra no se completa, debes saber que no podrás presentar ninguna reclamación.

PayPal no protege las compras a menos que se trate de transacciones de bienes o servicios.

- **Premios / Loterías**

Cada vez son más frecuentes los mensajes SMS / WhatsApp en los que se te pide que pagues una pequeña comisión de gestión a cambio de magníficos premios, viajes o estancias en resorts: por lo general, se trata de una estafa. Después de pagar lo solicitado mediante transferencia bancaria, tarjeta regalo o criptomoneda (sistemas de pago seguros para los delincuentes), no recibes nada.

No envíes dinero a nadie que no conozcas. Recibir un premio es gratis, siento desilusionarte, pero te has topado con un estafador.



- **Phishing:**

Es un tipo de estafa que se lleva a cabo en Internet y mediante la cual un delincuente intenta engañar a la víctima para que le facilite información personal, datos financieros o códigos de acceso, haciéndose pasar por una entidad fiable en una comunicación digital.

El término phishing es una variante de fishing (literalmente «pescar» en inglés) y alude al uso de técnicas cada vez más sofisticadas para «pescar» datos financieros y contraseñas de un usuario.

Por lo general, se recibe en el buzón de correo electrónico (e-mail) o a través de SMS falsos un aviso de actividad anómala detectada en la cuenta corriente. Estos correos electrónicos y SMS se caracterizan por la presencia de un enlace que redirige a un sitio web clonado del banco. Si se introducen los datos solicitados, el estafador tiene pleno acceso a la cuenta bancaria de la víctima.

Siempre hay que prestar atención a las siguientes señales que pueden ayudarte a detectar las estafas de phishing:

- Ningún banco enviaría nunca enlaces de acceso directo a su cuenta corriente online o a una página en la que introducir sus datos personales y bancarios. Es mejor desconfiar de estos comunicados y, en caso de duda, verificarlo con el centro de asistencia de su entidad bancaria.
- Muchos mensajes de phishing están mal redactados y pueden contener errores ortográficos, tipográficos y gramaticales.
- Los correos electrónicos y mensajes fraudulentos probablemente le redirigirán a un sitio web no seguro, por lo que siempre debe comprobar la URL y la ortografía del nombre de la empresa.
- No abras correos electrónicos que contengan archivos adjuntos, ya que pueden contener virus que infectarán tu dispositivo.



- ***Vishing:***

Es una estafa similar al phishing, que se aprovecha de la mayor confianza que las personas tienen en el contacto humano, pero el objetivo es idéntico, es decir, obtener información privada mediante engaños, utilizando el teléfono. El operador pide a la víctima que facilite sus datos, como el nombre de usuario y el PIN. Se recomienda interrumpir inmediatamente la llamada.

- ***Smishing:***

El smishing se diferencia del phishing en que se utilizan mensajes de texto convincentes en SMS que inducen a los destinatarios, gracias a un enlace presente en el mensaje, a enviar la información privada solicitada o a descargar programas maliciosos en el ordenador o el smartphone.

- ***Pharming:***

Un ataque informático cuyo objetivo es el robo de datos personales. El estafador dirige a la víctima a un sitio web «clon» con un nombre de dominio oficial equipado para robar los datos personales de la víctima o instalar malware en el ordenador del usuario, con el fin de obtener información personal y financiera.

Es un ataque muy difícil de detectar, ya que los ciberdelincuentes atacan el DNS (servidor de nombres de dominio) con el que consiguen redirigir a los usuarios a un sitio web falso.

NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS



- **Troyanos (Trojan):**

El término «troyanos» se refiere al malware de acceso remoto, que se instala en el ordenador de la víctima. El malware agrupa decenas de subcategorías (**Trojan-Proxy, Keylogger Trojans, Trojan-Spy**, etc.) con un único denominador común: robar los datos confidenciales almacenados en los ordenadores.

Los troyanos no se propagan por sí solos, a menudo es la propia víctima la que, sin darse cuenta, al no prestar atención a los correos electrónicos que recibe o a los sitios web que visita, descarga un troyano en su ordenador. Recientemente se han identificado virus troyanos en archivos con extensión PDF.



- **Recaudación de Fondos (Fake Crowdfunding)**

El crowdfunding no es más que una recaudación de fondos que se inicia generalmente para hacer frente a emergencias médicas y sanitarias, incluso tras un terremoto o una inundación, o para financiar a personas, fundaciones o asociaciones con el fin de llevar a cabo proyectos meritorios.

La estafa involucra a tres sujetos: el donante, el receptor y el delincuente. Este último retransmite o altera las comunicaciones entre las dos partes; concretamente, desvía los fondos hacia su propia cuenta corriente abierta en bancos extranjeros. A menudo, esta estafa va precedida de ataques troyanos o de phishing.

*Estos ataques informáticos, ya provengan de un correo electrónico, una llamada telefónica o un SMS, sustituyen a una comunicación oficial de una entidad estatal o una empresa importante y tienen un objetivo común: engañar al destinatario **para extorsionarle datos sensibles y acceder a su cuenta corriente y tarjetas de crédito.***

Aquí tienes algunos consejos para evitarlo:

1. No confíes nunca en solicitudes sospechosas: si alguien te pide información personal por correo electrónico o SMS, ¡mantente alerta!
2. Comprueba las direcciones y el lenguaje: los estafadores suelen utilizar direcciones de correo electrónico extrañas y tienen una gramática desastrosa.
3. Activa la autenticación de dos factores: así, aunque alguien consiga robar tus credenciales, necesitará un código que solo tú puedes tener.
4. Ponte en contacto directamente con la entidad: si recibes una comunicación extraña, ponte siempre en contacto directamente con la entidad utilizando los números oficiales.

Recuerda, ¡más vale prevenir que curar! Mantén tus datos a salvo y ten cuidado con a quién le das acceso a tu información. **Con un poco de precaución, podrás navegar por el mundo digital sin sorpresas desagradables!**



El engaño con el rostro de un familiar

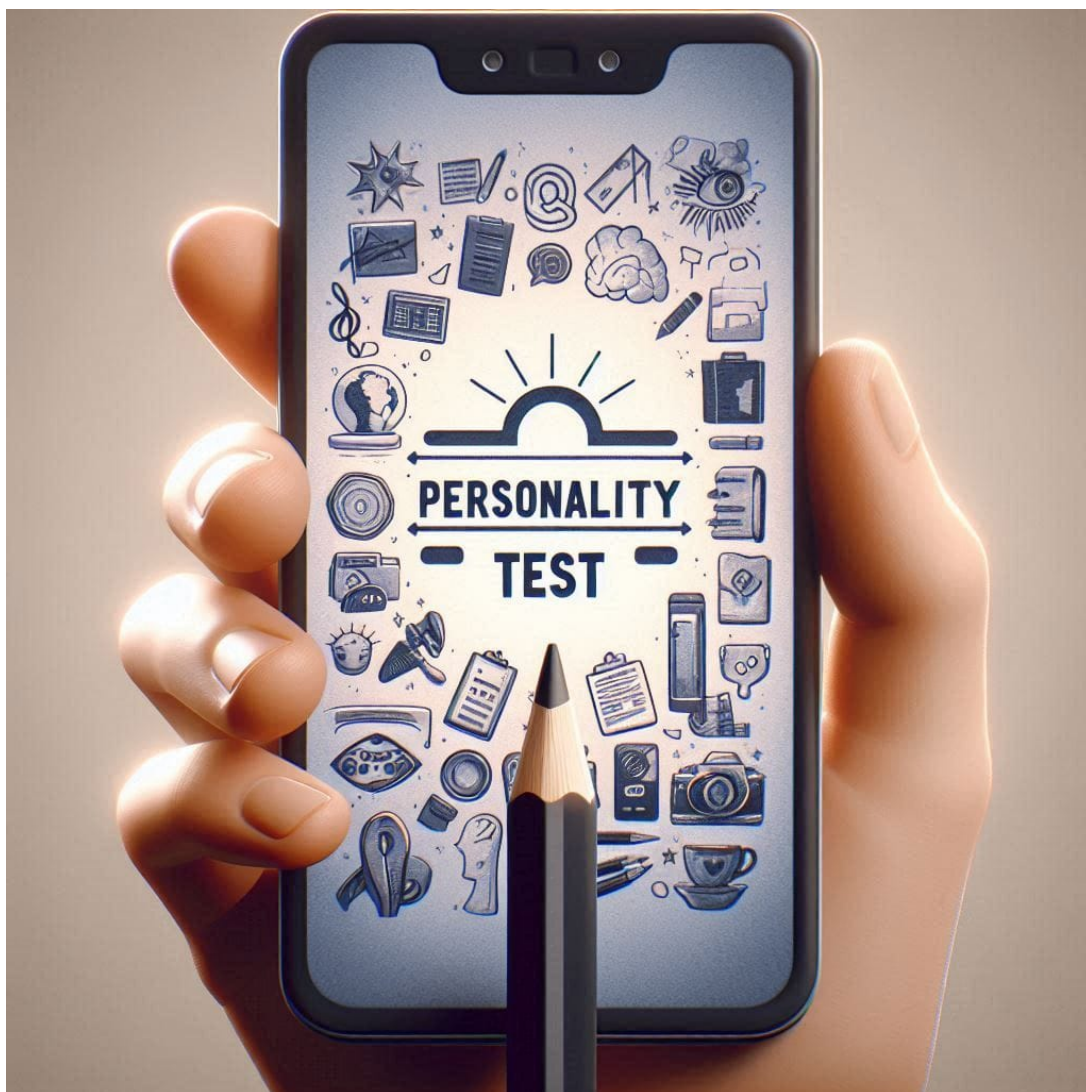
Imagina que un día cualquiera recibes un mensaje en tu smartphone que te deja sin palabras. Un vídeo inquietante aparece en la pantalla, y lo primero que ves es el rostro de tu hijo o nieto. Parece estar viviendo una pesadilla; está en apuros, rodeado de extraños que le gritan y se ríen de él. Tu corazón se detiene, la ansiedad te oprime el estómago.

No estás solo. En los últimos meses, las estafas alimentadas por la inteligencia artificial han aumentado de forma desmesurada. Las tecnologías avanzadas permiten manipular imágenes y sonidos, creando situaciones tan realistas que parecen verdaderas. Sin embargo, lo que estás viendo no es más que una simulación injusta, una distorsión de la realidad orquestada por personas malintencionadas.

Los delincuentes informáticos han descubierto cómo engañar a las familias y a las personas mayores aprovechándose de nuestra vulnerabilidad emocional. Utilizan software de deepfake para crear vídeos o fotos en los que superponen los rostros de familiares en escenas alarmantes. ¿Su objetivo? Extorsionar dinero o información confidencial, mientras las víctimas se ven atrapadas en una espiral de miedo y pánico. Pero no te dejes abrumar. Lo más importante es mantener la calma. Comprueba siempre la información antes de reaccionar. Ponte en contacto directamente con tu hijo o con cualquier persona que conozcas para confirmar que está bien. Recuerda que la verdad puede distorsionarse fácilmente en un mundo dominado por la tecnología.

En este contexto, es fundamental reconocer las señales de alerta y saber cómo defenderse de estas estafas. Solo así podremos esperar reducir el número de familias afectadas por este horrible engaño.

En un mundo en el que nada parece seguro, la concienciación es nuestra mejor arma. Actúa, infórmate y comparte estas experiencias. Solo así podremos construir una comunidad más fuerte y resistente, capaz de afrontar los retos del futuro. Y, en caso de duda, llama al **112**.



Juegos, concursos y pruebas en línea

En el vasto y fascinante mundo de los juegos en línea, donde la competición se mezcla con la diversión, se esconde una sombra insidiosa: las estafas. Este universo virtual, que promete aventuras extraordinarias y recompensas increíbles, atrae a millones de jugadores, muchos de los cuales desconocen los riesgos que corren. A menudo se trata de pruebas virales en Facebook, Instagram o sitios aparentemente inofensivos. Te piden acceso a tus perfiles o te llevan a páginas que imitan sitios web oficiales.

Se presentan en forma de cuestionarios, juegos o tests de personalidad, y a menudo tienen como objetivo:

1. Recopilar datos personales (nombre, edad, correo electrónico, ubicación, etc.).
2. Hacer que hagas clic en anuncios engañosos o enlaces fraudulentos.
3. Suscribirte sin saberlo a servicios de pago.
4. Robarte información para usos ilícitos (acceso a redes sociales, cuentas diversas).

Esempi comuni:

- Ejemplos comunes:
- «¡Descubre quién te ama en secreto!»
- «¿Qué tipo de personalidad tienes? ¡Responde a 5 preguntas para descubrirlo!»
- «¿Qué animal eres en tu vida pasada?»
- «¡Mira qué pasa si introduces tu nombre!» "Scopri chi ti ama in segreto!"

Cómo reconocer una estafa disfrazada de prueba/juego:

- No confíes en los enlaces compartidos en redes sociales o aplicaciones de mensajería.

Comprueba la URL: ¿es un dominio oficial o una página extraña llena de anuncios?

- No introduces datos personales sensibles para pruebas triviales;

Evita aceptar accesos con Facebook o Google si no estás seguro de la página.

Desconfía si al final te piden el número de teléfono o la tarjeta de crédito;

Bloquea y denuncia las páginas que te parezcan sospechosas.

**¡Si tienes alguna duda, no dudes en llamar al
NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS**



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>



Estafa del trabajo falso

Las ofertas de trabajo falsas en Internet son una de las estafas más comunes en los últimos años. Se presentan como anuncios atractivos, a menudo con salarios altos, poca experiencia requerida y la posibilidad de trabajar desde casa. En realidad, sirven para robar datos personales, hacerte pagar por «cursos» o «activaciones», o involucrarte en actividades ilegales como el blanqueo de dinero.

1. Cómo reconocer una estafa de oferta de trabajo falsa:

2. Prometen ganancias muy altas y fáciles

«¡Gana 3000 € (tres mil) al mes trabajando 2 horas al día desde casa!».

3. No piden cualificaciones ni experiencia

«No necesitas CV, ¡te contratamos inmediatamente!».

4. Se ponen en contacto contigo a través de WhatsApp, Telegram o correo electrónico personal. A menudo con mensajes mal redactados o genéricos.

5. Piden dinero por adelantado.

«Ingresa 50 € para activar la cuenta de trabajo».

«Tienes que comprar el kit inicial».

6. Quieren datos confidenciales con demasiada rapidez.

NIF, documento de identidad, número de cuenta.

7. La página web es extraña o poco profesional.

Comprueba si tiene errores, si falta una sede legal o un número de IVA.

8. Proponen «tareas» ambiguas o sospechosas.

Como recibir transferencias y transferirlas a otros (¡blanqueo de dinero!).



1. Ejemplos de estafas comunes:

- **«Trabajo como comprador misterioso» que requiere un pago inicial.**
- **«Trabajo en Amazon o Poste Italiane», pero desde correos electrónicos no oficiales.**
- **«Introducción de datos o paquetes», cuando en realidad quieren tu IBAN.**
- **Estafas a través de Telegram/WhatsApp en las que te piden que hagas clic en un enlace de «registro».**

2. Cómo protegerse

- Comprueba siempre la empresa en Google o LinkedIn.
- Nunca envíes dinero para conseguir un trabajo.
- Utiliza solo portales fiables como LinkedIn, InfoJobs, Indeed, etc.
- Si alguien se pone en contacto contigo, pide la sede, **el número de IVA y un contrato por escrito.**
- Denuncia las estafas a la Policía Postal: <https://www.commissariatodips.it>

Siempre mantén una actitud escéptica: en un mundo en el que la diversión puede convertirse en una estafa, la prudencia es tu mejor aliada. Jugar es divertido, pero hacerlo de forma segura es aún mejor!

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.

- El falso CUP

A veces todo empieza con una llamada o un mensaje que parece provenir del servicio sanitario, con un tono urgente que habla de una visita o una cita que hay que confirmar e invita a volver a llamar inmediatamente a un número.

La palabra «urgente» suele bastar para provocar la prisa, sobre todo si se está esperando una respuesta, y se vuelve a llamar sin pensarlo dos veces.

Al otro lado, sin embargo, no hay un operador sanitario, sino una línea que permanece en espera con mensajes o música mientras la llamada continúa y se agota el saldo. Incluso unos pocos minutos pueden suponer una pérdida sin que llegue nunca una respuesta real.

Funciona porque aprovecha el momento de las prisas, cuando se actúa antes de verificar.

Por eso la regla es sencilla: nunca llames al número indicado en el mensaje o en la llamada. Para cualquier verificación, utiliza siempre y solo los canales oficiales del servicio sanitario, como la página web institucional, el CUP de tu ASL o el médico de cabecera.

Si ya has llamado, ponte en contacto con tu operador telefónico para comprobar si hay servicios de pago y desactivarlos.

Si has facilitado datos personales, contraseñas, PIN o enviado documentos, actúa de inmediato: interrumpe todo contacto y denuncia lo ocurrido al 112 para recibir asistencia.

Los expertos aconsejan llamar a tu operador y solicitar la desactivación del servicio VAS. El siguiente paso es presentar un formulario de reclamación ante el CoReCom (Comité Regional de Comunicaciones, órgano dependiente de la Agcom).



Si tienes la más mínima duda, no dudes en llamar al

NÚMERO ÚNICO EUROPEO DE EMERGENCIAS 112

Puedes utilizar el portal oficial de la Comisaría de Policía Online,
rellenando el formulario de la sección «Denunciar online»

<https://www.commissariatodips.it>

El SPID «invisible»

Imagina que utilizas tu SPID como lo haces todos los días, para acceder a los servicios en línea, consultar tus datos, comprobar una notificación o quizá esperar un reembolso, sin que nada parezca fuera de lugar, porque todo funciona exactamente como siempre.

Es precisamente esta normalidad la que hace que bajemos la guardia, porque no hay nada que haga pensar que algo haya cambiado.

Sin embargo, en algunos casos, alguien podría haber conseguido utilizar tus datos personales para activar un segundo SPID a tu nombre, mientras que el tuyo sigue funcionando sin problemas y sin dar ninguna señal.

Dos identidades digitales que no se ven entre sí.

Y a través de ese acceso paralelo es posible entrar en los portales oficiales, consultar información y, en algunas situaciones, llegar incluso a modificar datos sensibles como el IBAN, con la consecuencia de que los posibles pagos pueden tomar un camino diferente al previsto.

La particularidad de esta situación es que no ocurre nada evidente de inmediato, porque todo sigue funcionando con normalidad, sin avisos ni señales claras, hasta el momento en que algo no cuadra, quizá precisamente cuando no llega un pago esperado.

Y a menudo es solo entonces cuando uno se da cuenta de que algo ha cambiado.

Por eso, de vez en cuando, es importante dar un paso atrás y revisar los propios datos, accediendo directamente a portales oficiales como el INPS o NoiPA, para comprobar que todo concuerda con lo que uno sabe, sin fiarse de las comunicaciones recibidas ni de las notificaciones inesperadas.

Al mismo tiempo, es fundamental no compartir nunca documentos personales o información sensible en respuesta a solicitudes repentinas, incluso cuando parezcan creíbles.

Porque en estos casos todo se reduce a un detalle muy sencillo: desde fuera no parece que esté pasando nada.

Y cuando surge la duda, aunque sea solo por un instante, ya es el momento de detenerse, comprobar con calma e intervenir de inmediato si algo no cuadra.

Habla con tus familiares o personas de confianza, tómate tu tiempo para comprobar tus datos y, si algo no cuadra, no esperes: compruébalo de inmediato y denuncia lo ocurrido.

Llama al 112 o señalar <https://www.commissariatodips.it>



El falso carabinero / agente de Hacienda / policía

En el pasado, estas llamadas solían empezar casi siempre de la misma manera: un hijo, un nieto o un familiar involucrado en un accidente, un problema repentino, la petición urgente de dinero que había que entregar de inmediato para resolverlo todo.

Hoy, en cambio, la historia cambia de forma y a menudo parece aún más creíble.

Suena el teléfono y, al otro lado, una voz se presenta con seguridad, dice ser un carabinero, un agente de Hacienda o un policía, y habla de un atraco, de un problema legal, de una transferencia urgente que hay que bloquear o de un incidente que afectaría a tu coche o al de un familiar, mientras tú aún intentas entenderlo y la conversación ya sigue adelante, como si algunos detalles se dieran por sentados.

A veces la historia cambia de nuevo y todo parte del supuesto hallazgo de un documento, una tarjeta o un objeto perdido, con la petición de confirmar datos personales que, en ese momento, parecen normales de comunicar.

La voz se mantiene tranquila, acompaña cada explicación sin levantar nunca el tono, hasta que llega la petición de revisar el dinero o las joyas, de prepararlos porque alguien pasará a verificarlos, como si fuera un procedimiento normal que hay que llevar a cabo sin perder tiempo.

Y es precisamente cuando todo parece discurrir sin interrupciones cuando algo, aunque sea solo por un instante, empieza a no encajar del todo.

Porque, más allá de la historia que se cuenta, estas situaciones casi siempre se basan en los mismos factores: las prisas, la confianza, la autoridad y el miedo a equivocarse precisamente en ese momento.

Y a menudo basta precisamente esa duda para interrumpir la llamada, tomar distancia de esa situación y sacar todo de esa presión que hasta hacía un momento parecía plausible.

En ese momento, verificar vuelve a ser algo que se hace con calma, usando otro teléfono o esperando unos minutos, y si alguien llama a la puerta es importante quedarse dentro, sin abrir.

Porque ninguna urgencia llega así.

Y cuando algo no convence, aunque sea solo por un momento, ya es hora de parar, hablarlo con alguien de confianza y denunciar lo ocurrido. Llama al 112.



- ¿Ladrones con el terminal de pago: realidad o exageración?

Imagina que estás en medio de la multitud, en el autobús, en el mercado o haciendo cola en el supermercado, en uno de esos momentos en los que la gente se mueve sin cesar y el contacto entre desconocidos se vuelve normal, casi inevitable, hasta el punto de que ya ni te fijas.

Alguien se acerca más de lo habitual, te roza el costado o la mochila, y por un instante todo se pierde en esa confusión de espacios estrechos y movimientos continuos.

Entonces te viene a la mente algo que oíste hace tiempo, la posibilidad de que existan dispositivos capaces de realizar pagos con solo acercarse a una tarjeta sin contacto, y a partir de ese momento, casi sin darte cuenta, empiezas a mirar a tu alrededor de otra manera.

Últimamente se ha hablado de los llamados carteristas con TPV, personas que utilizarían terminales portátiles para intentar realizar pagos acercándose a las víctimas.

La idea llama la atención precisamente porque parece algo que puede suceder sin que se note.

Sin embargo, en la realidad, se necesita una condición muy concreta, ya que el dispositivo debería estar prácticamente en contacto con la tarjeta y sin obstáculos, mientras que en la vida cotidiana la tarjeta casi siempre está dentro de una cartera, en un bolsillo o en un bolso, y esto lo hace todo mucho más difícil.

Por este motivo, este tipo de situaciones siguen siendo poco probables, mientras que el riesgo real es, con mucha más frecuencia, el que siempre hemos conocido: un carterito que te quitan, una mochila abierta, un momento de distracción en medio de la multitud.

Y es precisamente ahí donde conviene centrar la atención.

Comprueba siempre dónde guardas tus tarjetas, evita los bolsillos exteriores o las mochilas abiertas, activa las notificaciones de pago y, si detectas aunque sea una sola operación que no reconoces, no esperes: ponte en contacto inmediatamente con el banco y bloquea la tarjeta.

Porque, al fin y al cabo, no es tanto el escenario lo que marca la diferencia, sino la rapidez con la que se reacciona.

Y si algo no cuadra, aunque sea solo por un instante, compruébalo de inmediato, habla con alguien de confianza y no dudes en denunciarlo.



- El seguro demasiado barato

Cada vez es más habitual buscar seguros por Internet, quizá en cualquier momento del día, cuando se tiene un rato libre y se intenta averiguar si hay alguna forma de ahorrar sin renunciar a nada.

Entre los muchos sitios web que aparecen, hay algunos que resultan familiares de inmediato, con colores ya vistos, logotipos reconocibles y palabras que transmiten una sensación de seguridad, como si ya estuviéramos en el lugar adecuado sin necesidad de detenernos realmente a comprobarlo. Se introduce la matrícula casi sin pensarlo y, en pocos segundos, aparece una oferta que llama más la atención que las demás, porque promete la misma cobertura a un precio mucho más bajo, pero solo por un tiempo limitado, como si fuera una oportunidad que hay que aprovechar antes de que desaparezca.

Uno se detiene un momento a mirarla, mientras se va gestando la idea de que realmente puede ser un buen negocio, y justo en ese momento puede llegar también una llamada telefónica, con una voz tranquila y preparada que acompaña la elección sin forzar, pero dando a entender que esperar demasiado podría significar perder esa oportunidad.

Inmediatamente después llega un mensaje con un contrato, unos documentos, un enlace para completar todo, y cada elemento parece estar en su sitio, sin levantar sospechas evidentes, así que se sigue adelante, porque todo ha sido construido para parecer normal.

Pasan los días, pero no llega nada: ni una confirmación, ni un documento válido, ni una respuesta; el número ya no está disponible y la página web, al volver a buscarla, ya no existe. Y es solo en ese momento cuando queda claro que ese proceso tan lineal se había diseñado al detalle para conducir precisamente hasta allí, sin dejar señales evidentes por el camino.

Por eso, antes de llegar hasta el final, basta con detenerse un momento y salir de ese camino, verificando desde un punto externo, a través de los canales oficiales o contactando directamente con la IVASS al número gratuito 800 486661, porque a veces es precisamente ese pequeño control el que cambia completamente el rumbo.

Y si algo no cuadra, aunque solo sea por una sensación difícil de explicar, ya es el momento de detenerse, no seguir adelante y pedir consejo a alguien de confianza. **Habla con familiares o amigos, comprueba siempre antes de pagar y, si temes haber sido engañado, denuncia inmediatamente lo sucedido. Llama al 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.

La póliza de vida «segura»

Cada vez es más frecuente que nos contacten con propuestas que hablan de seguridad y protección, sobre todo cuando se refieren a los ahorros acumulados a lo largo del tiempo y al deseo de protegerlos frente a cualquier imprevisto.

La voz al otro lado se presenta con calma, sin prisas, con un tono que no presiona sino que acompaña, y describe una solución que parece pensada precisamente para dar tranquilidad, una póliza que protege y hace crecer el dinero sin exponerlo a riesgos.

Las palabras fluyen de forma lineal, sin suscitar dudas inmediatas, y en los días siguientes llegan también documentos, tablas, referencias a una compañía conocida, elementos que dan continuidad a esa primera impresión, como si todo siguiera un camino ya trazado.

Se escucha, se evalúa, y en un momento dado la elección parece natural, casi una consecuencia de lo que se ha dicho y mostrado, así que se firma, se paga, y durante un breve periodo parece que todo va bien.

Luego, poco a poco, algo cambia.

Las comunicaciones se interrumpen, el número ya no responde y, cuando se intenta verificar, sale a la luz lo que antes no era visible: esa póliza no existe, esa propuesta nunca fue real.

Solo entonces se recompone el panorama y se comprende que cada paso había sido construido para llegar hasta allí, sin crear nunca un momento evidente en el que detenerse.

Por eso, antes de llegar a ese punto, es importante dar un paso al margen de ese proceso y verificar la información a través de los canales oficiales, comprobando siempre que el intermediario y la compañía estén autorizados o contactando directamente con la IVASS al número gratuito 800 486661, ya que a menudo es precisamente esta comprobación la que cambia por completo el rumbo.

Y cuando surja la duda, aunque sea solo por un instante, ya es el momento de detenerse, no seguir adelante y consultar con alguien de confianza.

Habla con familiares o amigos, comprueba siempre antes de pagar y, si temes haber sido estafado, denuncia inmediatamente lo ocurrido.

Llama al 112.

**¡Si tienes alguna duda, no dudes en llamar al
NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS**



RECUERDE SIEMPRE QUE:

- Ninguna oficina pública o privada (INPS, INAIL, ASL, etc.) envía a sus empleados a domicilio para cobrar pagos, verificar facturas o controlar billetes y joyas.
- Ninguna empresa proveedora de luz, gas o agua solicita información sobre dinero o joyas.
- Ningún repartidor de paquetes, cartas certificadas u otra correspondencia se presenta en el rellano de su casa: la entrega se realiza en la puerta principal, en el vestíbulo del edificio o en el buzón.
- Si se ponen en contacto con usted alegando que su hijo o un familiar está en peligro (por ejemplo, en el hospital, involucrado en un accidente o detenido) y le piden dinero o joyas para ayudarlo, no se fíe: aunque la voz le resulte familiar, podría tratarse de un estafador.
- Si se presentan desconocidos en la puerta o llaman al interfono diciendo que pertenecen a las fuerzas del orden, o llevan uniformes y muestran tarjetas de identificación, gorras o paletas con símbolos oficiales, **no abra la puerta**. Compruebe desde el balcón o la ventana si hay un coche de servicio en la calle e intente averiguar el motivo de la visita.
- Si le piden que les deje entrar en su casa para revisar la instalación eléctrica, de gas o de agua, o para realizar reparaciones, **no abra la puerta** si no ha recibido una notificación oficial de la empresa proveedora del servicio. Compruebe siempre que haya un vehículo de la empresa fuera y, en caso de duda, póngase en contacto directamente con la empresa.

- No utilices números de teléfono proporcionados por desconocidos, aunque digan que quieren demostrar su identidad.
- Nunca facilites información personal a personas que no conozcas. Si te das cuenta de que la has compartido con un estafador, denúncialo inmediatamente para proteger tu identidad.

Para tu seguridad en línea

Si utilizas la banca online desde tu smartphone, protege siempre tus datos. Te recomiendo que utilices una cuenta de correo electrónico dedicada exclusivamente a las comunicaciones bancarias, distinta de la principal.

Cuando accedas a Internet, conéctate siempre a través de una VPN segura, evita las redes Wi-Fi públicas y ten cuidado con los códigos QR que escaneas.

- **Si eres víctima de una estafa, cuenta lo sucedido a tus amigos y familiares. Así evitarás que ellos también sean estafados.**

LLAMA SIEMPRE AL NÚMERO ÚNICO EUROPEO PARA EMERGENCIAS



AGRADECIMIENTOS

Un agradecimiento especial a las personas que me han apoyado en la realización de este vademécum:

a la Secretaria General Stefania Castricone y a la secretaría del Si.Na.Fi.

(Sindicato Nazionale de Finanzas) por su patrocinio gratuito;

a Christian Diana, director general de la «Anglo American Academy» de Cagliari, por su patrocinio gratuito;

al Dr. Antonio Pirro, Agente General de la Agencia Generali Cagliari Porto, por su patrocinio gratuito;

al artista Francesco Mascia Cogoni por las espléndidas ilustraciones realizadas con Microsoft Designer y al amigo Luca Meloni por las espléndidas ilustraciones realizadas con Microsoft Designer, Gemini, Flow, Chatgpt;

al Dr. Roberto Borghetti y al Dr. Matteo Capaldo del Grupo Trizio;

al Dr. Gennaro Fuoco por el tiempo que me ha dedicado;

a mi amigo Luca Agati por su confianza constante;

al Dr. Alberto Covini por su amable apoyo.

A Officine Grafiche della Sardegna S.r.l. – (CA) por la sensibilidad demostrada.

Además, deseo expresar una mención especial y un sincero agradecimiento a «Striscia la Notizia» y a todos sus colaboradores y corresponsales. Gracias a su incansable compromiso y a la dedicación con la que abordan temas relevantes y de actualidad, el programa destaca por el papel fundamental que desempeña en la vigilancia de las estafas, tanto en el territorio como en el mundo digital.

Las secciones no solo informan al público sobre las trampas más comunes, sino que también ofrecen consejos prácticos sobre cómo prevenir posibles estafas. En una época en la que el fraude adopta nuevas formas y métodos cada vez más sofisticados, la capacidad de «Striscia la Notizia» para sacar a la luz estos problemas supone un valioso servicio para la comunidad.

A través de un lenguaje accesible y reportajes incisivos, el programa guía a los ciudadanos hacia una mayor concienciación y una mejor preparación contra las estafas. Gracias a estos esfuerzos, muchos pueden sentirse más seguros y protegidos, sabiendo que pueden contar con una información clara y directa.

Seguridad de las cuentas en línea: una protección que nunca debe subestimarse

Hoy en día utilizamos Internet para muchas cosas importantes.

Con unas sencillas precauciones es posible proteger mejor tus cuentas.

- **Utiliza contraseñas seguras**

La contraseña debe ser larga y difícil de adivinar.

Es importante utilizar contraseñas diferentes para cada servicio.

Por ejemplo:

la contraseña del banco no debería ser la misma que la del correo electrónico o las redes sociales.

- **Activar la verificación mediante código**

Muchos sitios web, además de la contraseña, solicitan también un código que se recibe en el teléfono. Esto ayuda a proteger la cuenta aunque alguien descubra la contraseña.

- **Mantener actualizados el teléfono y el correo electrónico de recuperación**

El número de teléfono y el correo electrónico deben estar siempre correctos y operativos.

Sirven para recuperar la cuenta si se pierde la contraseña o ya no se puede acceder a ella.

- **Guarda los códigos de emergencia**

Algunos servicios proporcionan códigos especiales que debes guardar en un lugar seguro.

Pueden ayudarte a volver a acceder a la cuenta en caso de problemas.

- **Utiliza herramientas de protección adicionales**

Existen aplicaciones o pequeños dispositivos que aumentan la seguridad de las cuentas.

Todas estas medidas de protección deben revisarse de vez en cuando.

Incluso un número de teléfono antiguo que ya no se utilice puede crear problemas a la hora de recuperar la cuenta.

La seguridad en línea depende de muchos pequeños detalles que, en conjunto, ayudan a proteger los datos y la información personal.

Si eres víctima de una estafa, cuenta lo que te ha pasado a tus amigos y familiares. Así evitarás que ellos también sean estafados.

APOYO GRATUITO OFRECIDO POR



© Cavoli Sergio 2025 – “Guía contra el fraude: juntos somos más fuertes”

www.infotruffe.com

Licenza: Creative Commons BY-NC-ND 4.0 International

Uso permitido: citar al autor, no modificar, no utilizar con fines comerciales.

Enlace a la licencia: <https://creativecommons.org/licenses/by-nc-nd/4.0/>