Truffe e raggiri in rete

(e per strada)

Sicurezza, tutela della privacy e uso consapevole della rete

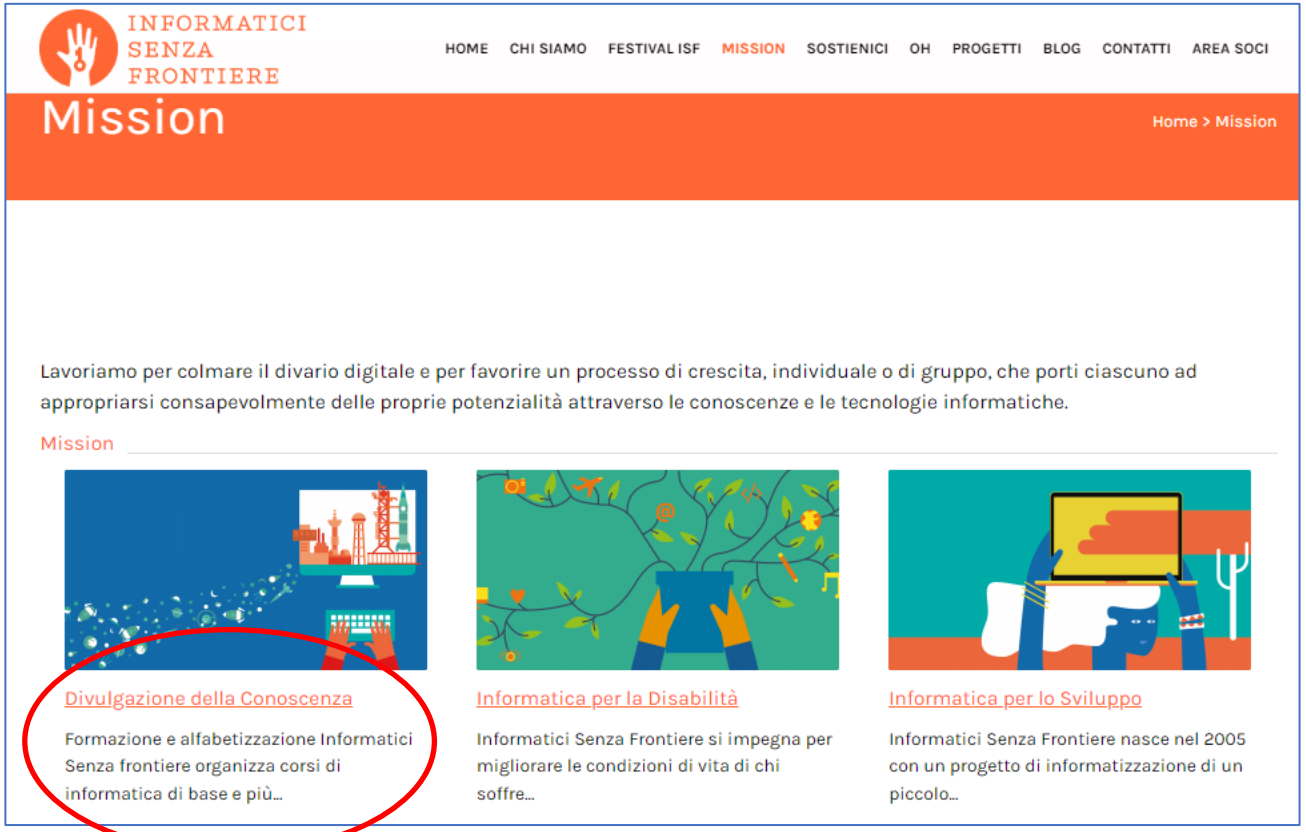
Montebelluna, 22 maggio 2024

Maurizio Tosatto

maurizio.tosatto@informaticisenzafrontiere.org

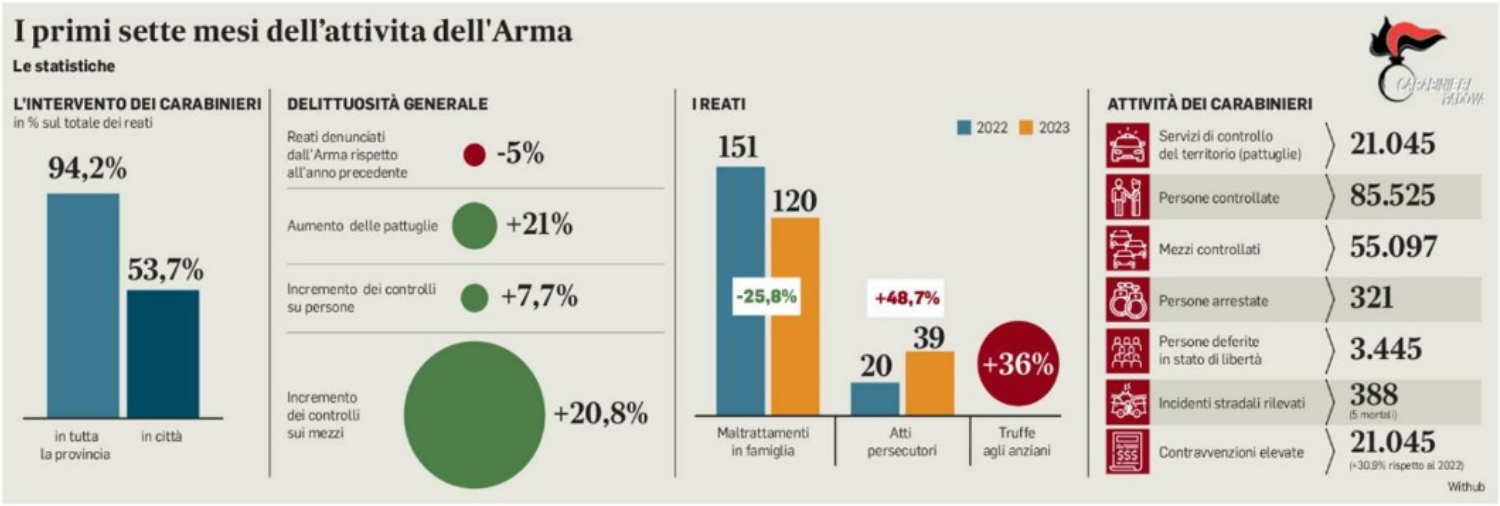
Informatici senza Frontiere, chi siamo…

INFORMATICI SENZA FRONTIERE



Tra le sue molteplici attività, ISF realizza e propone corsi di informatica di base per ridurre il "digital divide", cioè aiutare chi è poco competente nell'uso di strumenti informatici o chi li sa usare ma non ne percepisce i limiti, ad usarli al meglio.

Truffe, un allarme sociale!!!!



Reati in calo, ma crescono stalking e truffe ad anziani

Le truffe, in particolare alle persone anziane, sono aumentate del 36% e costituiscono preoccupante fenomeno di allarme sociale…

Per contrastarlo la cosa più importante è l'informazione!

Truffe al telefono: lo schema

- Si riceve una telefonata, chi chiama si qualifica come un "avvocato".
- Vi avvisa che un figlio o un nipote è nei guai, il più delle volte per un incidente, ma anche un arresto, e vuole aiutarlo in via confidenziale. Non dovete chiamarlo, dovete tenere la linea libera.
- Vi viene chiesto del denaro, una cifra molto alta per es. 10.000€, ma arrivano anche a 50.000€ e se non l'avete anche gioielli e oggetti di valore che servono da cauzione e verranno stimati da un "perito" a casa vostra.
- Viene spiegato che c'è un danno da risarcire, ci sono stati feriti, e si deve fermare il procedimento. Viene chiesto un numero di telefono per essere chiamati da un maresciallo o un funzionario.
- Subito dopo che avrete acconsentito arriverà il "perito", "maresciallo" o "avvocato", per ritirare denaro e preziosi sparendo nel nulla!

Truffe al telefono

«Sua figlia ha investito un bimbo». Ma è una truffa

▶Scoperto il finto perito: in cella un 20enne napoletano

CRIMINALITÀ

PADOVA Una donna disperata che chiede aiuto e un ragazzo visto fuggire da un condominio in zona Sacra Famiglia: questa la scena descritta al 113 da un residente che ieri, poco dopo le 12, ha contattato la linea di emergenza.

Due Volanti hanno individuato un giovane che alla vista degli agenti entrava in una strada privata chiusa da una sbarra e, intuendo che potesse trattarsi della persona segnalata, lo hanno fermato. Il ragazzo, 20enne napoletano, ha sin da subito cercato di giustificare la sua presenza in quel luogo dicendo di essere lì perché alla ricerca di un lavoro.

Gli operatori, accertato che poco prima era stata consumata una truffa ai danni di una 66enne della zona, hanno invece capito che si trattava proprio dell'uomo che cercavano.

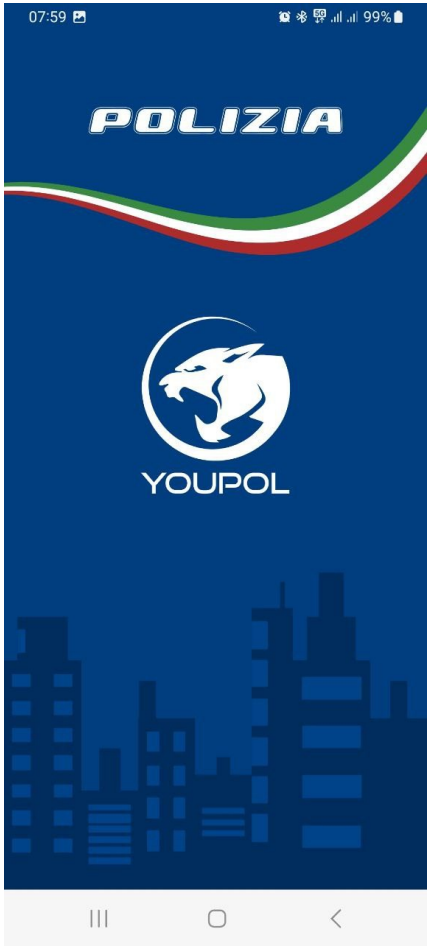
Sottoposto al controllo, all'interno dello zainetto che aveva con sé, hanno trovato un sacchetto con gioielli e orologi che il ragazzo sosteneva di aver preso da sua madre per affrontare il viaggio. Riconosciuto dalla vittima come autore della truffa, è stato arrestato e portato d in carcere.

L'uomo era entrato nell'abitazione della vittima che, tenuta costantemente al telefono da un finto maresciallo, era stata convinta a consegnare tutti i valori che aveva per "salvare" la figlia coinvolta in un incidente in cui avrebbe investito una mamma con un passeggino.

Il finto maresciallo le aveva detto che sarebbe arrivato da lei un perito per valutare i preziosi. Ma la donna, una volta visto il ragazzo, aveva intuito che non poteva trattarsi di un perito. Il malvivente, dopo averla spinta a terra, si era introdotto nella casa sottraendo il sacchetto preparato con i gioielli.

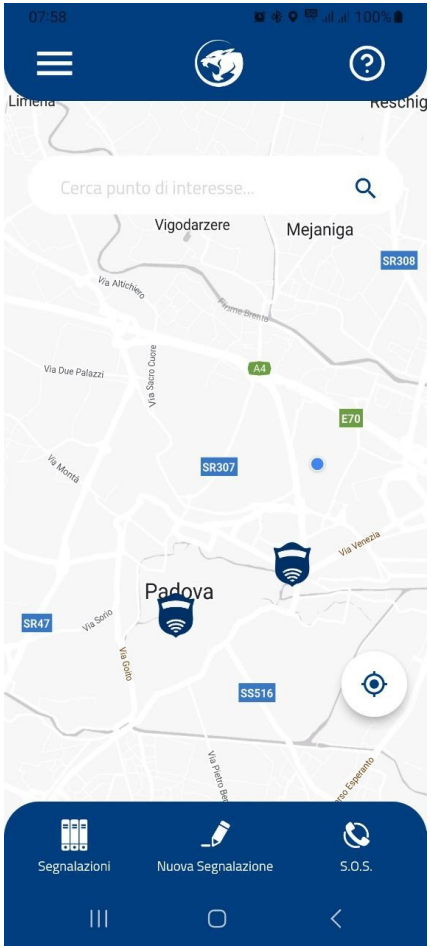
L'INTERVENTO La polizia ha rintracciato il malvivente

«Esprimo – ha dichiarato il Questore – la mia più profonda soddisfazione per l'arresto dell'autore dell'ennesima truffa ai danni di anziani. Mi sono immediatamente rallegrato con il dirigente dell'Ufficio Volanti, Valeria Pace, con gli Ispettori Coordinatori e con gli Agenti che hanno effettuato l'arresto».



YOUPOL l'app della Polizia di Stato

- Disponibile sia per telefoni Android che per Apple/iOS
- Semplice da usare
- Permette di segnalare velocemente situazioni di emergenza o chiedere soccorso dando tutte le informazioni necessarie



Numero Unico Emergenza

Sicurezza digitale

Tipologia di minacce alla sicurezza e alla privacy:

- **Tecnologiche**, ovvero mirate più propriamente alle componenti hardware e software dei dispositivi.
  - Relativamente facile contrastarle perché la tecnologia è intrinsecamente (quasi) sicura
  - Importante seguire alcune regole per mantenere un elevato standard di sicurezza

- **Comportamentali**, ovvero attività atte a indurre le persone a compiere azioni o a rivelare informazioni personali in maniera inconsapevole
  - L'elemento umano è l'anello debole della catena della sicurezza

Difendersi dalle minacce comportamentali

- Le minacce comportamentali agiscono sul nostro stato emotivo alterandolo, possiamo provare:
  - disagio -> preoccupazione -> paura -> panico
  - sorpresa -> contentezza -> euforia
- Lo scopo evidente è indurre una risposta irrazionale per farci trascurare o sottovalutare un rischio
- Se avvertiamo un'alterazione del nostro stato d'animo dobbiamo evitare di prendere subito decisioni:
  - Meglio aspettare di recuperare la serenità
  - Il confronto con un'altra persona può essere di aiuto
- Infatti spesso la minaccia si presenta come una drammatica e/o urgente emergenza

Sicurezza digitale: minacce tecnologiche

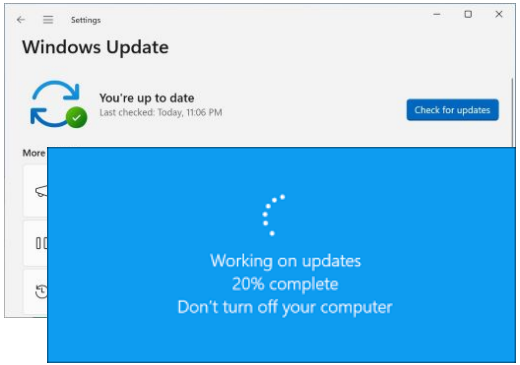
INFORMATICI SENZA FRONTIERE

- **Virus, Trojans, Worm, Spyware**: sono programmi o “pezzi” di codice che vengono inseriti all’interno di altri programmi e possono carpire informazioni, infettare altri PC tramite mail, provocare malfunzionamenti o eseguire attacchi di tipo distruttivo (es. Ransomware).
- **Phishing e SMiShing** : uso di e-mail o SMS ingannevoli e di falsi siti Web per indurre gli utenti a fornire informazioni confidenziali o personali

Consigli di protezione (1)

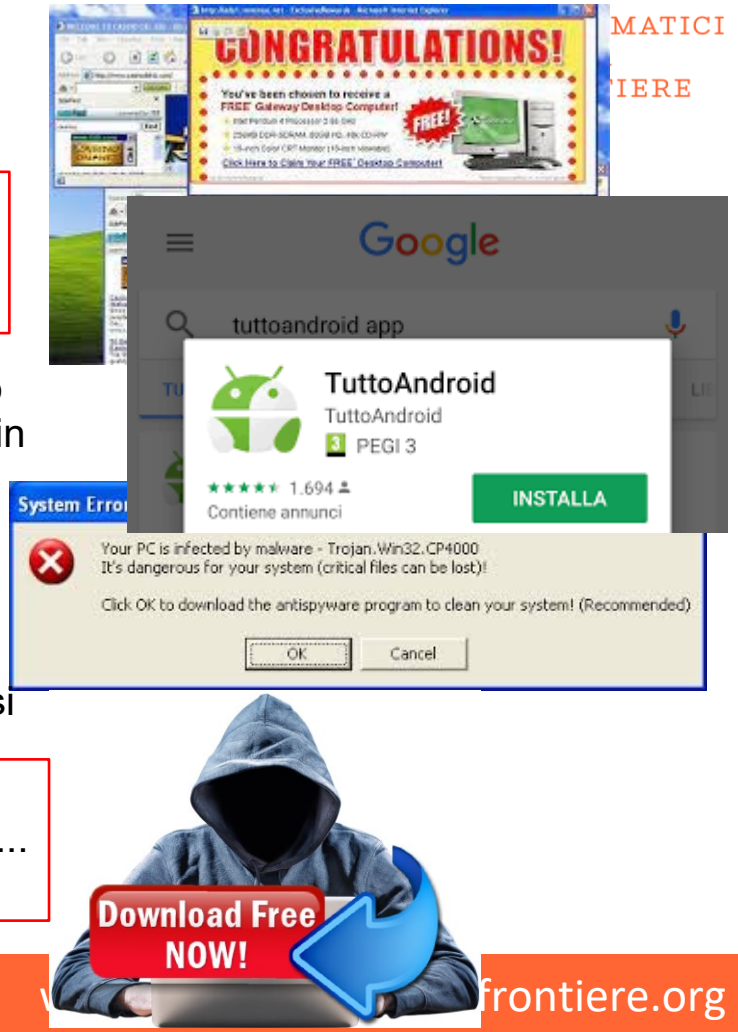
INFORMATICI SENZA FRONTIERE

- Usate un software **antivirus** con aggiornamenti automatici
- Usate un **firewall** (filtro di rete) sui computer collegati a Internet
- Effettuare sempre gli **aggiornamenti** dei sistemi operativi e dei programmi/app installati
- Effettuate **backup** regolari dei programmi e dei dati (USB drive 512GB/15-20€, ma usatelo solo sul vostro PC!)
- Non tenete il computer acceso collegato alla rete quando non lo usate (oltretutto è anche poco ecologico!!)
- Verificate che la **connessione sia protetta**. Se il sito che visitate si trova su un server protetto, il collegamento deve iniziare con **https://** Inoltre verificate che ci sia l'icona del **lucchetto chiuso** nella barra dell'indirizzo (URL) del browser

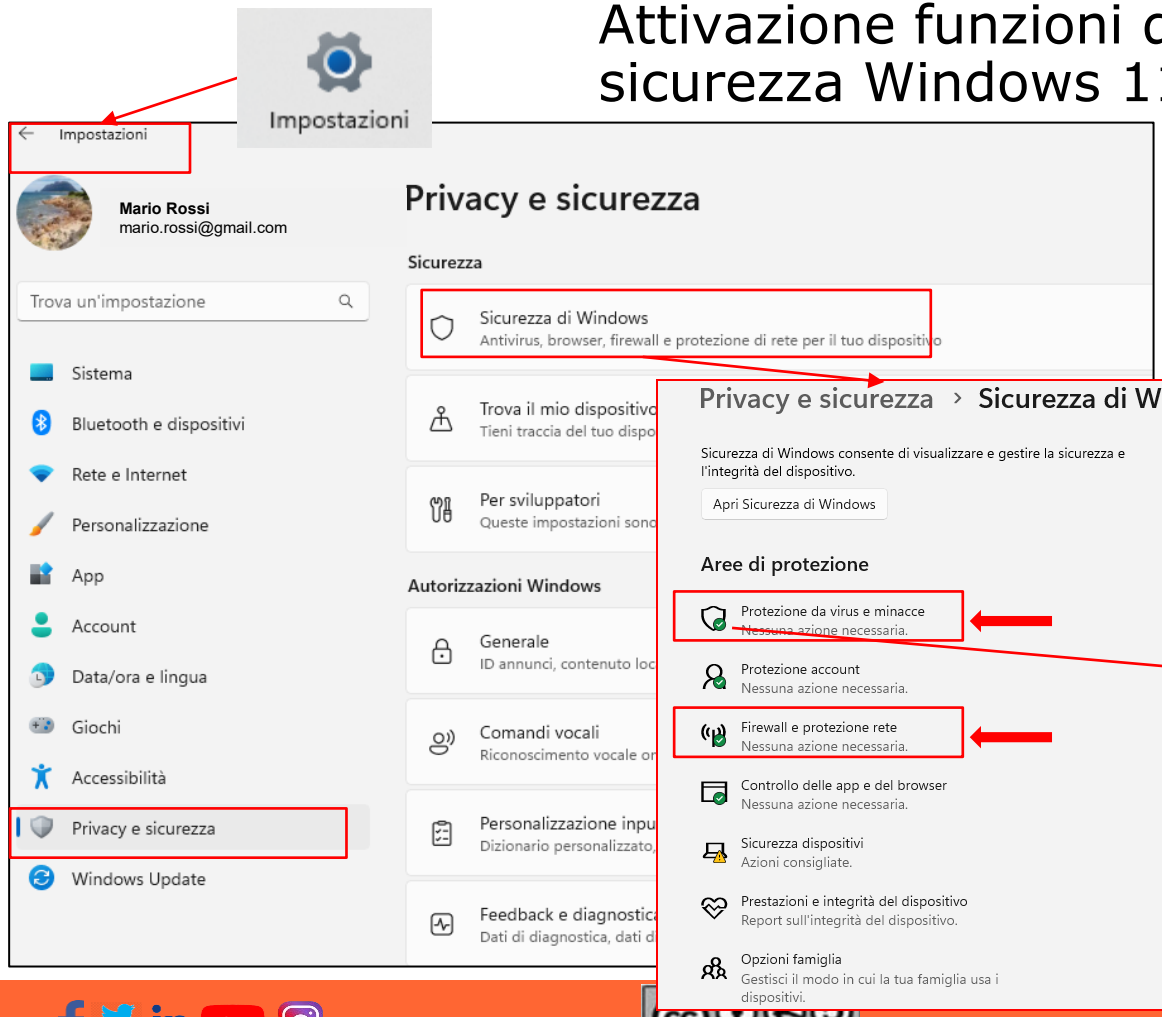


Consigli di protezione (2)

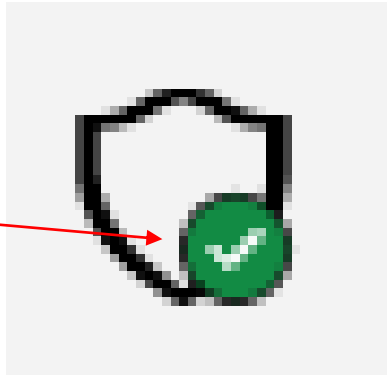
- Non inserite PIN/Password e dati personali su pc ad uso pubblico o connessi a reti pubbliche (WiFi al bar o in aeroporto) in particolare se aperte (no password)
- Valutate l'uso di una **VPN** (connessione criptata gratuita o a pagamento) che permette di non apparire direttamente in Internet
- Non cliccate sulle **finestre popup,** specialmente se avvertono della presenza di virus sul computer e offrono soluzioni, non selezionate il link e non autorizzate nessun download. Potreste scaricare e installare software dannosi
- Non usate versioni gratuite "craccate" di programmi a pagamento, potrebbero contenere virus, spyware, trojans... Oltretutto è un reato!



Attivazione funzioni di sicurezza Windows 11

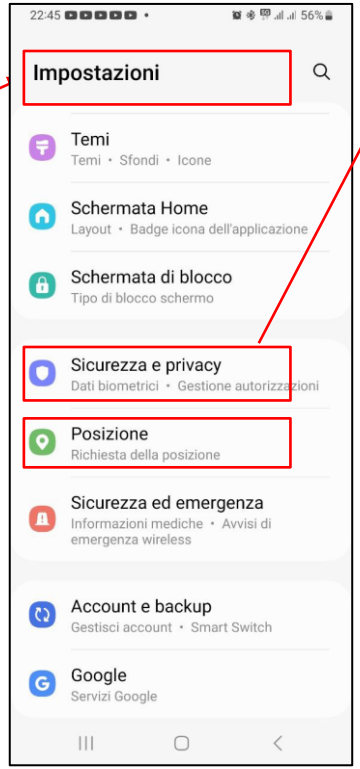


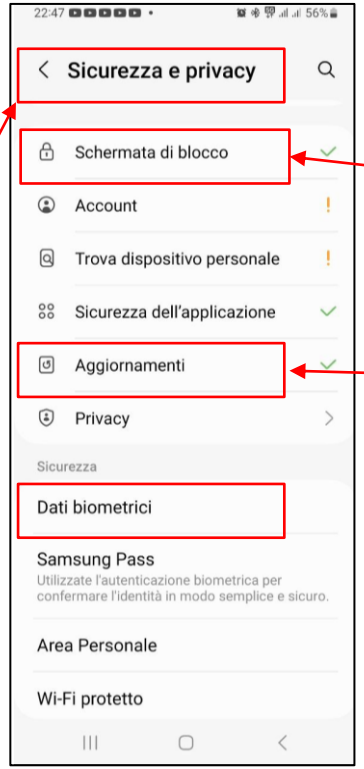
Se le opzioni di sicurezza hanno il bollino verde significa che sono attive e aggiornate



Attivazione funzioni di sicurezza ANDROID

INFORMATICI SENZA FRONTIERE





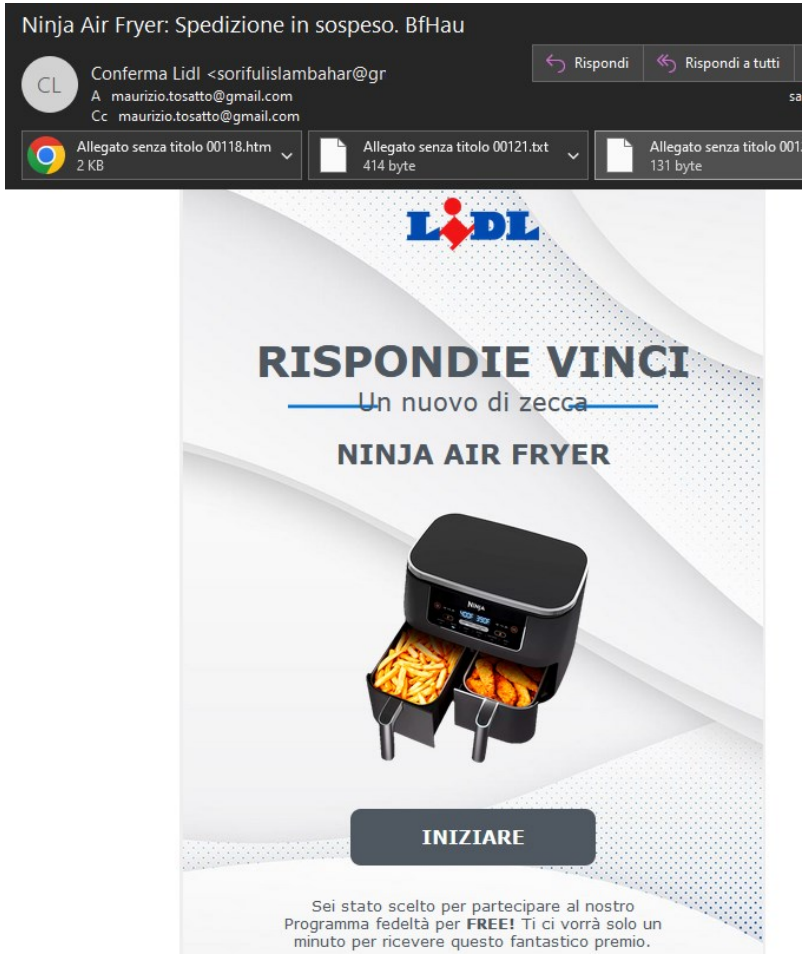
- Le funzioni di sicurezza standard sono sufficienti per il controllo del dispositivo
- Come per il PC è sempre bene avere almeno un **PIN per l'attivazione dello schermo**, indispensabile se lo si usa per i pagamenti
- E' opportuno personalizzare alcune funzioni come la possibilità di **aggiornamento anche tramite la rete telefonica** per chi non ha il WiFi a casa.

Sicurezza digitale: Phishing e SMiShing

INFORMATICI SENZA FRONTIERE

Esempio di email **phishing** che simula la richiesta da parte di un corriere, BRT, di informazioni per la consegna di un pacco. Cosa fare?

- Prima di tutto domandiamoci se stiamo aspettando un pacco… no? Problema risolto! Ci rimane un dubbio?
- Ci deve insospettire lo stranissimo indirizzo del mittente
- Un'altra cosa dubbia è l'indirizzo che compare passando (senza cliccare) col mouse sopra all'area che ci dovrebbe farci navigare sul sito.
- Un controllo sul sito BRT https://www.brt.it/it/ permette di capire subito che non è attinente.
- Di solito chiedono il pagamento di pochi € per carpire dati bancari
- La maggior parte di queste mail viene filtrata dal sistema di posta e messa nello SPAM



Sicurezza digitale: Phishing e SMiShing

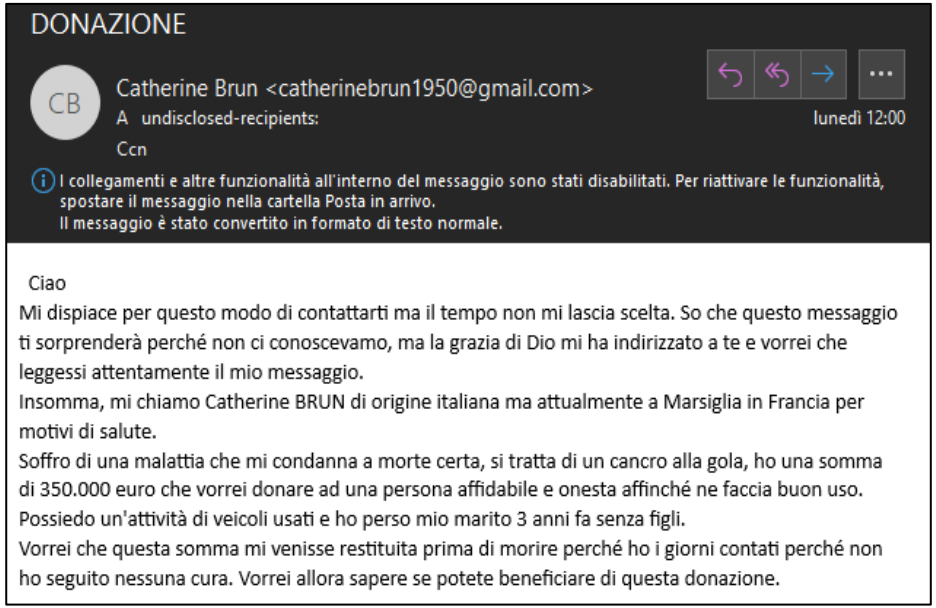
INFORMATICI SENZA FRONTIERE

Esempio di email phishing che propone una vincita.

- Il mittente è un qualunque indirizzo gmail
- È scritto male e con errori
- QUESTO E' GIA' SUFFICIENTE PER DUBITARE
- Cliccando su INIZIARE (non fatelo) si viene inviati su un sito che non ha niente a vedere con LIDL. Ogni ulteriore click è pericoloso!!!
- Non aprite MAI gli allegati di un messaggio dubbio!

Sicurezza digitale: Phishing e SMiShing

INFORMATICI SENZA FRONTIERE


DONAZIONE

CB

Catherine Brun <catherinebrun1950@gmail.com>

A undisclosed-recipients:

Ccn

lunedì 12:00

I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo.
Il messaggio è stato convertito in formato di testo normale.

Ciao
Mi dispiace per questo modo di contattarti ma il tempo non mi lascia scelta. So che questo messaggio ti sorprenderà perché non ci conoscevamo, ma la grazia di Dio mi ha indirizzato a te e vorrei che leggessi attentamente il mio messaggio.
Insomma, mi chiamo Catherine BRUN di origine italiana ma attualmente a Marsiglia in Francia per motivi di salute.
Soffro di una malattia che mi condanna a morte certa, si tratta di un cancro alla gola, ho una somma di 350.000 euro che vorrei donare ad una persona affidabile e onesta affinché ne faccia buon uso.
Possiedo un'attività di veicoli usati e ho perso mio marito 3 anni fa senza figli.
Vorrei che questa somma mi venisse restituita prima di morire perché ho i giorni contati perché non ho seguito nessuna cura. Vorrei allora sapere se potete beneficiare di questa donazione.

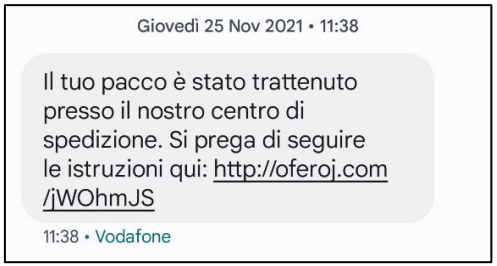
Esempio di email phishing che propone la donazione di una somma importante.

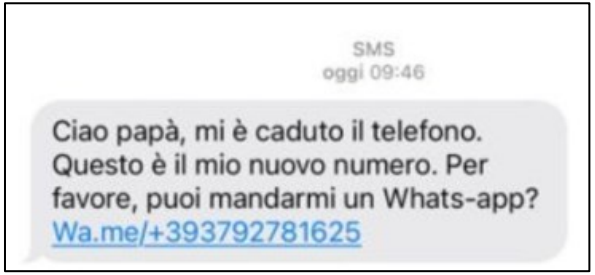
Cosa pensare?

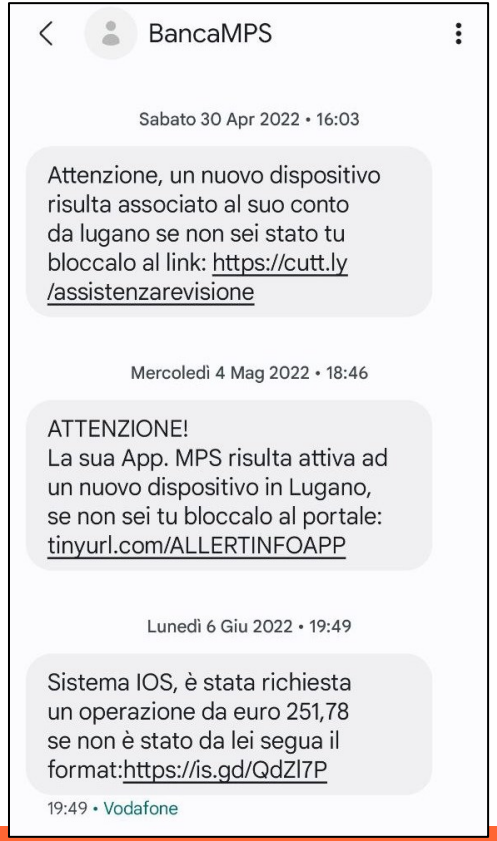
- Il mittente è sconosciuto ma lo ammette lei stessa ed essendo quasi straniera giustifica il pessimo italiano. La malattia aggiunge drammaticità. Sembrerebbe plausibile ma…
- Ci deve insospettire che non abbia nessuno a cui donare una somma così importante a fin di bene, in altri casi viene proposta un'eredità, un compenso per un aiuto o una vincita ad una lotteria.
- Rispondere a questo messaggio non è pericoloso in se, ma rischiate di farvi coinvolgere con metodi molto persuasivi.
- L'evoluzione tipica è che vi viene chiesta una somma di poche centinaia di euro per “gestire la pratica”. Ovviamente poi la donazione non arriva…

Sicurezza digitale: Phishing e SMiShing

INFORMATICI SENZA FRONTIERE







Esempi di SMS fraudolenti.

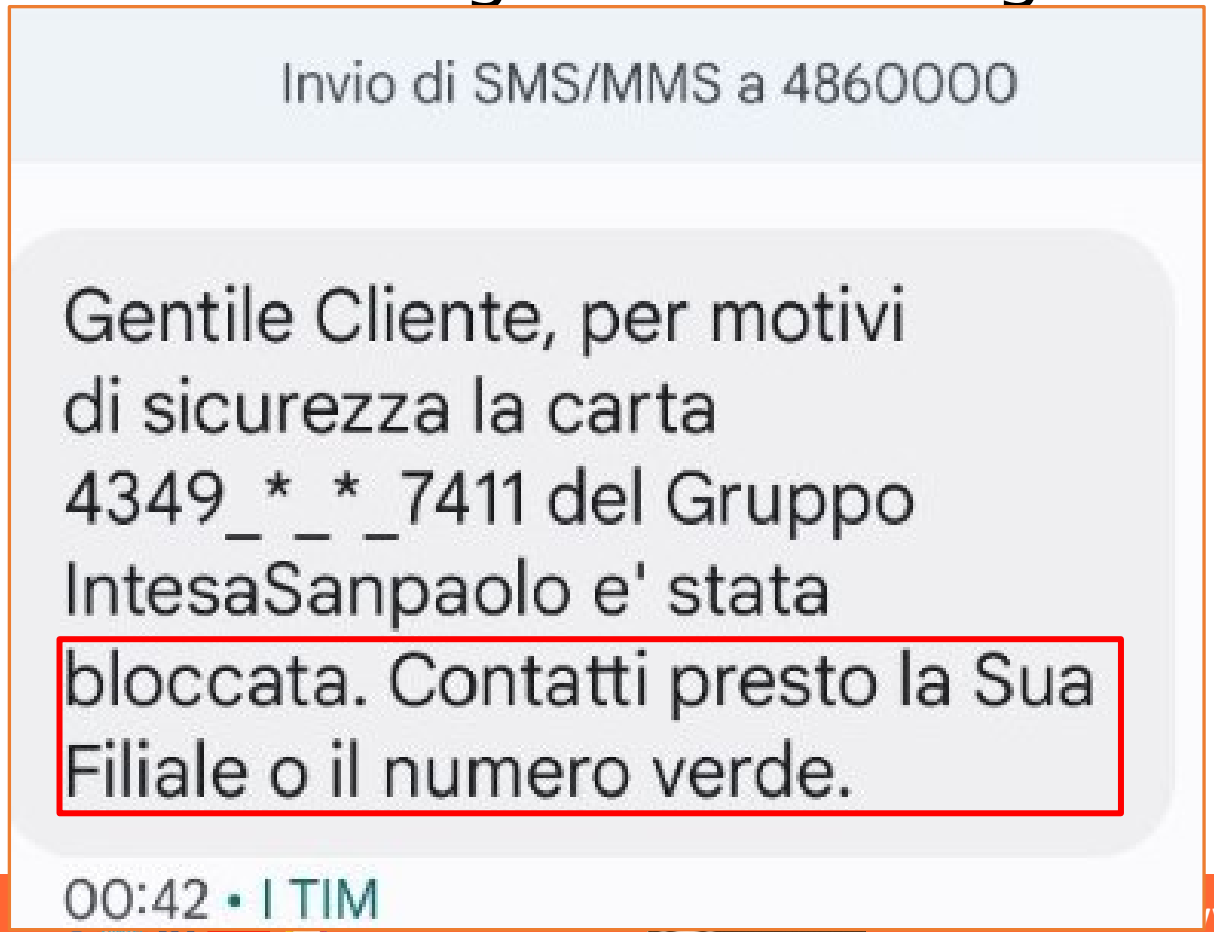
Simulano problemi con consegne, allarmi per tentativi di accesso, richieste da parenti o difficoltà con conti correnti bancari, addirittura anche proposte di investimenti o pagamenti di multe stradali.

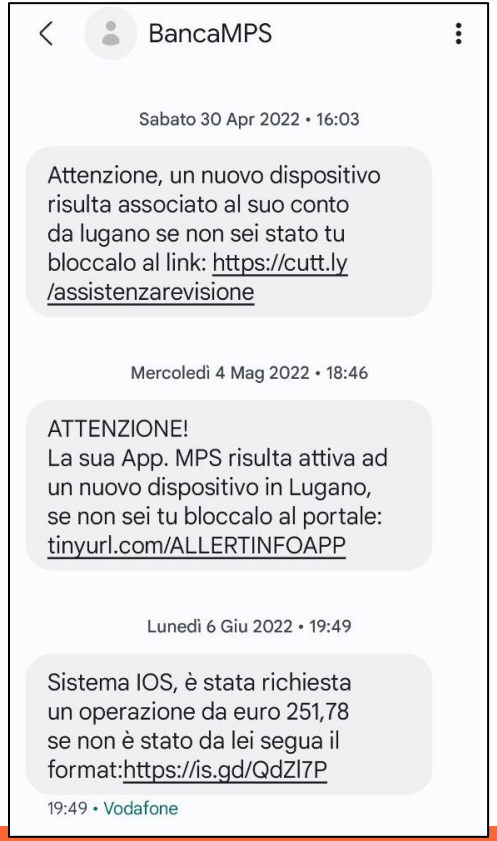
Non devono essere presi in considerazione, **mai cliccare sui link**!

Se avete dubbi contattate l'ente mittente tramite canali ufficiali o recatevi allo sportello della vostra banca

Sicurezza digitale: Phishing e SMiShing

INFORMATICI SENZA FRONTIERE





Mettiti alla prova!

INFORMATICI SENZA FRONTIERE

https://phishingquiz.withgoogle.com

Siti fasulli: assicurazioni RCA on-line

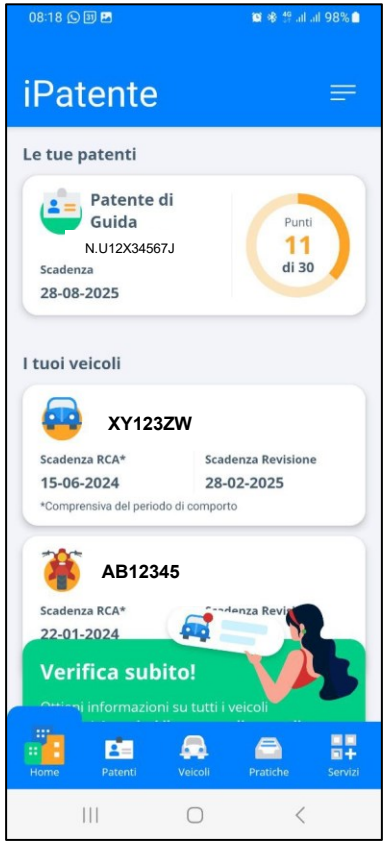
INFORMATICI SENZA FRONTIERE

- È risaputo che le assicurazioni on-line sono in generale più economiche, ma attenzione!!!
- Chiunque può "inventare" un assicurazione e relativo sito web!
- Solo quelle vigilate dall'IVASS (ex ISVAP) sono valide.
- Verifica l'iscrizione agli albi dell'IVASS dell'impresa e dell'intermediario: https://www.ivass.it/consumatori/proteggi/index.html
- In caso di dubbi chiamare l'IVASS al **numero verde gratuito 800 486661** da lunedì a venerdì (8:30 - 14:30).
- Dopo aver stipulato verifica sempre la copertura assicurativa tramite www.ilportaledellautomobilista.it oppure tramite l'app **iPatente** (accesso tramite SPID o CIE)

IVASS ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

iPatente
www.ilportaledellautomobilista.it

App iPatente



- Disponibile sia per telefoni Android che per Apple/iOS
- Accesso tramite SPID/CIE
- Permette di avere le informazioni su:
  - Scadenza propria assicurazione
  - Scadenza revisione
  - Scadenza e punti patente
  - Verifica assicurazioni altrui

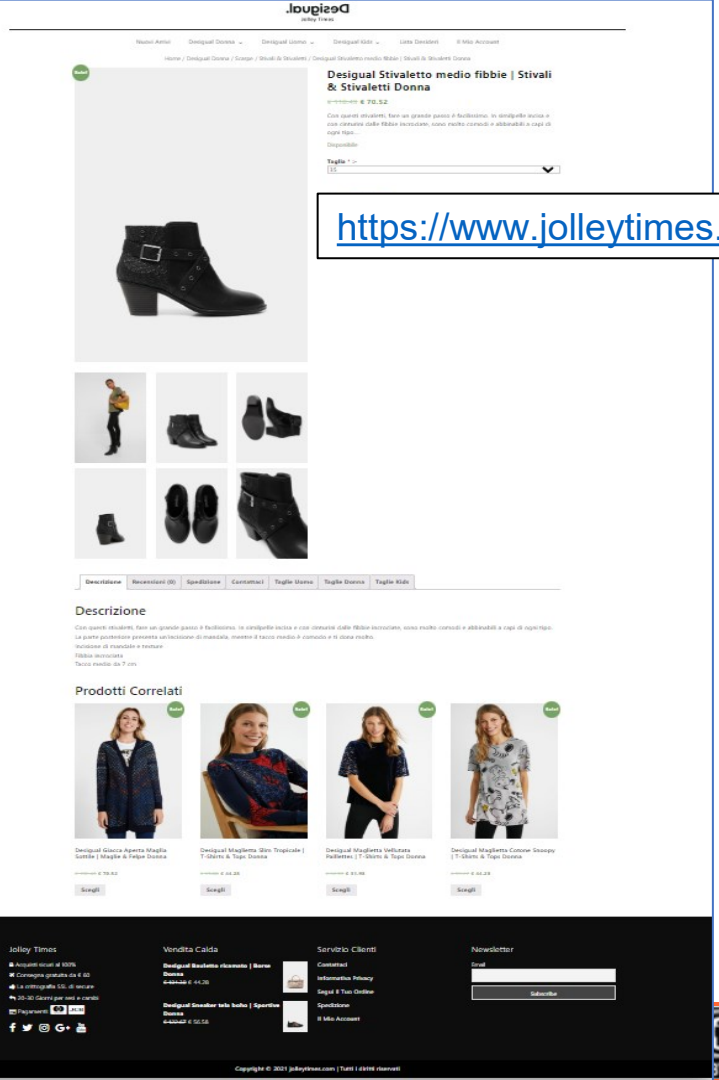
Siti fasulli: investimenti on line

INFORMATICI SENZA FRONTIERE

- Il fai date per investire i propri risparmi può essere pericoloso!
- Chiunque può "inventare" un sito che promette elevati rendimenti per attirare investimenti!
- Una delle truffe più ricorrenti riguarda l'acquisto di azioni di società famose come AMAZON o APPLE tramite canali incontrollabili.
- Solo le istituzioni finanziarie vigilate dalla CONSOB sono autorizzate in Italia, sul loro sito ci sono più pagine sulle truffe e abusi che riportano siti/aziende segnalate:
  - https://www.consob.it/web/area-pubblica/occhio-alle-truffe
  - https://www.consob.it/web/investor-education/truffe
- Consob ha oscurato parecchie centinaia di siti dal 2019

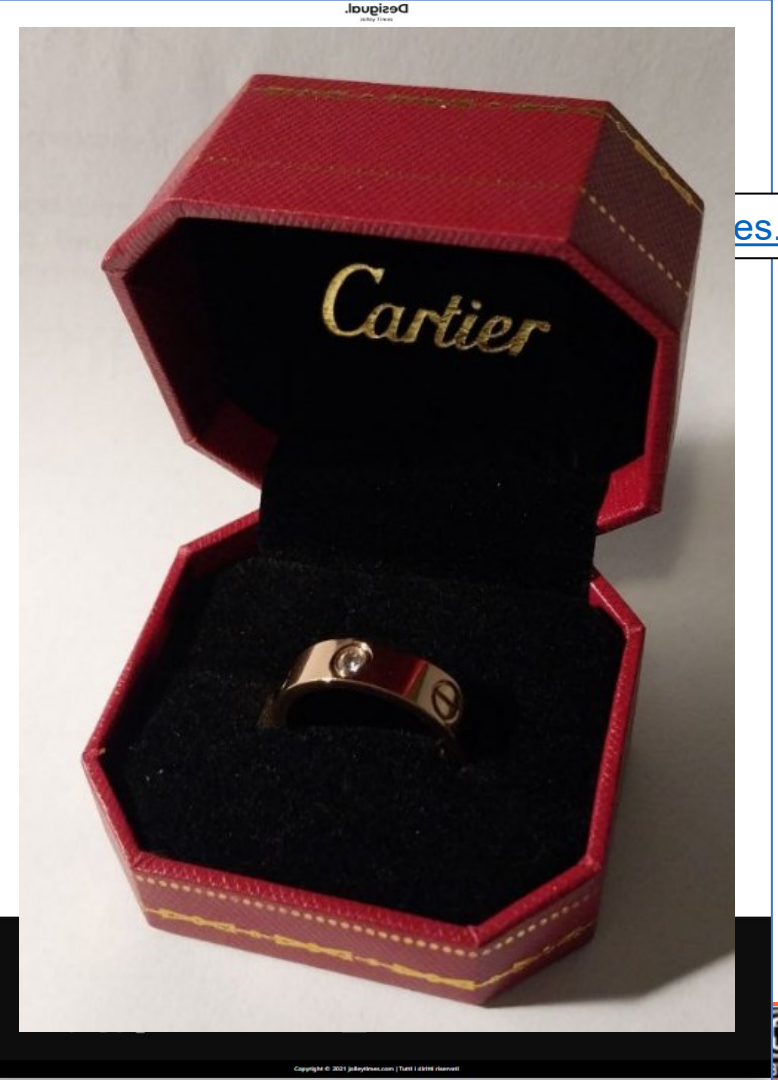
CONSOB

Acquisti on line…



https://www.jolleytimes.com/saldi/desigual-stivaletto-medio-fibbie-stivali-stivaletti-donna/

- Il sito non è quello della marca dei prodotti (?!?!)
- Manca ogni riferimento ad una sede, (sono in Europa?)
- Le condizione di vendita sono generiche
- Se provate a scrivere al "contatto" ricevete un messaggio di errore
- I link ai social (FB, Twitter/X, Instagram…) non portano alle pagine del venditore
- Potreste non ricevere nulla o una brutta sorpresa!!!
- Appena vi accorgete della truffa bloccate subito la carta di credito!



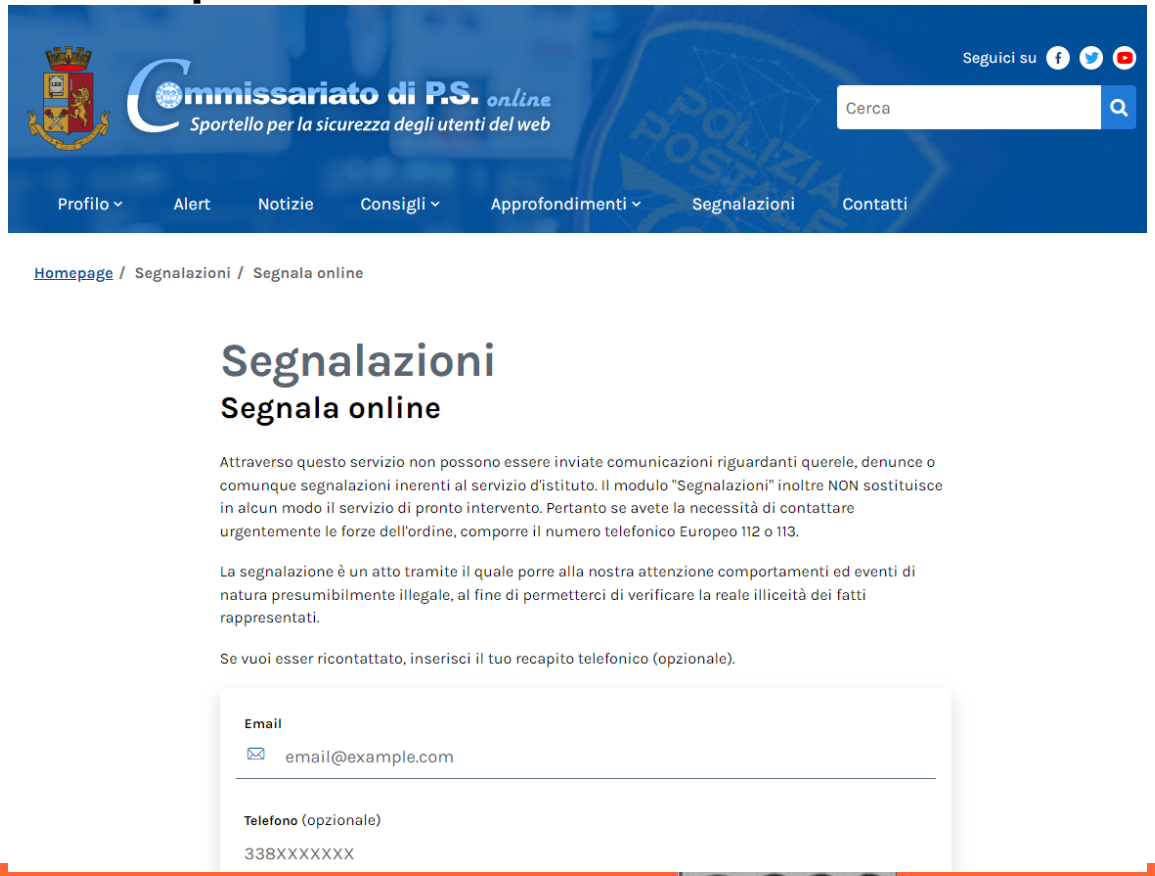
Acquisti on line…

INFORMATICI SENZA FRONTIERE

es.com/saldi/desigual-stivaletto-medio-fibbie-stivali-stivaletti-donna/

- Il sito non è quello della marca dei prodotti (?!?!)
- Manca ogni riferimento ad una sede, (sono in Europa?)
- Le condizione di vendita sono generiche
- Se provate a scrivere al "contatto" ricevete un messaggio di errore
- I link ai social (FB, Twitter/X, Instagram…) non portano alle pagine del venditore
- Potreste non ricevere nulla o una brutta sorpresa!!!
- Appena vi accorgete della truffa bloccate subito la carta di credito!

Acquisti on line…



- Cosa posso fare?
- Segnalare il sito alla polizia postale: www.commissariatodips.it
- Formalizzare una denuncia per truffa entro tre mesi recandovi in questura o dai carabinieri
- Dopo la riforma Cartabia i reati contro il patrimonio non sono più perseguibili d'ufficio ma solo su querela

Acquisti on line…

INFORMATICI SENZA FRONTIERE

Fare acquisti on-line in sicurezza si può! Basta seguire alcune regole:

- Scegliete piattaforme e-commerce note e di provata affidabilità
- Verificare l'attendibilità del sito e-commerce sconosciuto, fate ricerche in rete
- Diffidare di prezzi troppo bassi -> confrontare più piattaforme
- Verificare in rete le recensioni di altri utenti sia per quel prodotto che per il sito
- Non fare acquisti tramite dispositivi di altri (i dati sono memorizzati!)
- Diffidare di siti con errori di grammatica o strafalcioni grossolani
- Verificare attentamente le condizioni di vendita e di consegna
- Verificare termini e procedure per il recesso e clausole di garanzia
- Per il pagamento usare metodi sicuri (carte di credito ricaricabili o usa e getta, PayPal, …), evitate di memorizzare carte di credito nei siti e-commerce. L'importo addebitato sulla carta di credito deve coincidere

Che cos'è il furto di identità?

- Il furto di **identità digitale** avviene impadronendosi delle credenziali di accesso ad un sito o di info bancarie in modo da poter operare al posto di un'altra persona.
- Avviene tramite **navigazione imprudente** in internet con dispositivi non protetti da antivirus e firewall su reti non sicure come WiFi pubblici, spesso a causa phishing
- Le conseguenze possono arrivare alla perdita del **denaro sul conto**, del controllo sui propri **social** e degli account sui siti di **e-commerce** e della **pubblica amministrazione** (es. INPS, Ag. Entrate)

Consigli per le password

Le password più diffuse?

- 123456, password, qwerty, …

Le password rischiano:

- di essere indovinate
- di essere sbirciate
- essere intercettate
- essere spiate (spyware, trojan…)

Chi conosce la password di un utente può rubargli l'identità per quel sito! Meglio usare password lunghe (>10) e complesse (numeri, minuscole, maiuscole e simboli)

	abc Pass 323548 unique values	123 Frequency 1 4,115
1	123456	4,115
2	12345	1,281
3	123456789	753
4	juventus	704
5	000000	618
6	andrea	596
7	francesco	544
8	napoli	532
9	giuseppe	507
10	antonio	486
11	ciccio	438
12	12345678	438
13	111111	434
14	amore	412
15	alessandro	409
16	francesca	376
17	stella	354
18	amoremio	353
19	123	348
20	valentina	336
21	password	328
22	libero	327

Consigli per le password: password manager

INFORMATICI SENZA FRONTIERE

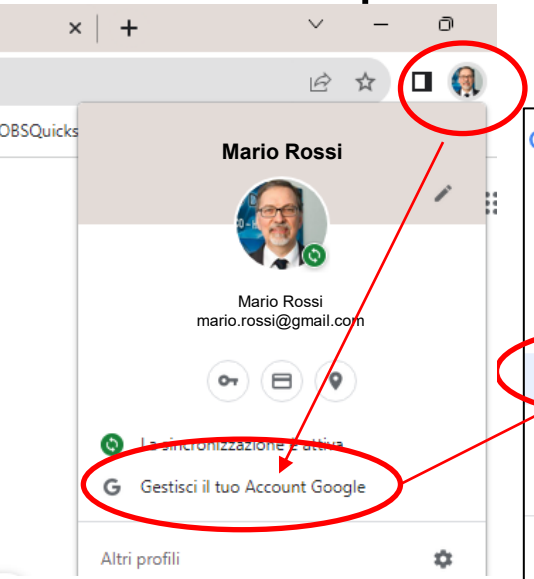
- Risolvono il problema di dover ricordare le password lunghe e complesse
- **Gratuiti**: KeePass, Bitwarden, Sophos Intercept X for Mobile
- **A pagamento**: LastPass, 1Password, Dashlane, Keeper
- **Integrati nel browser**: Safari, Google Chrome, Mozilla Firefox, Microsoft Edge
- E se la dimentico o la perdo? Ci sono sempre metodi per il recupero delle password!

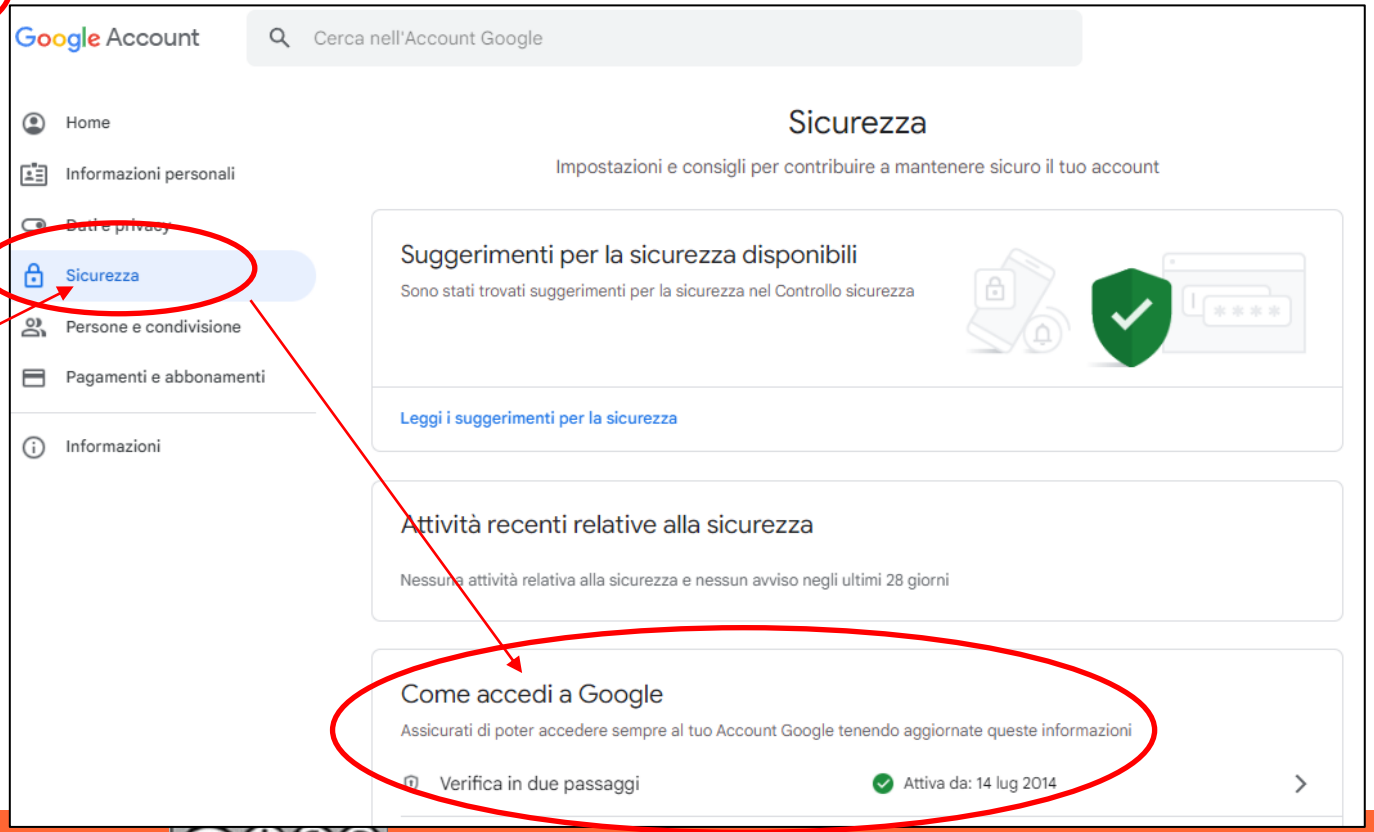
L’autenticazione a due fattori (2FA)

INFORMATICI SENZA FRONTIERE

- Migliora enormemente la sicurezza dell'accesso rispetto alla sola password, è richiesto dalla normativa UE per tutti i siti bancari/finanziari.
- **L’autenticazione a due fattori** usa due diversi metodi di autenticazione, in pratica ti verrà chiesto:
  - Chi sei (**UserID**, spesso si usa l'indirizzo email)
  - Una cosa che sai solo tu (**password**)
  - Una cosa che puoi avere solo tu (**telefono, smart card, dati biometrici**)

Esempio di autenticazione a due fattori: l'account Google

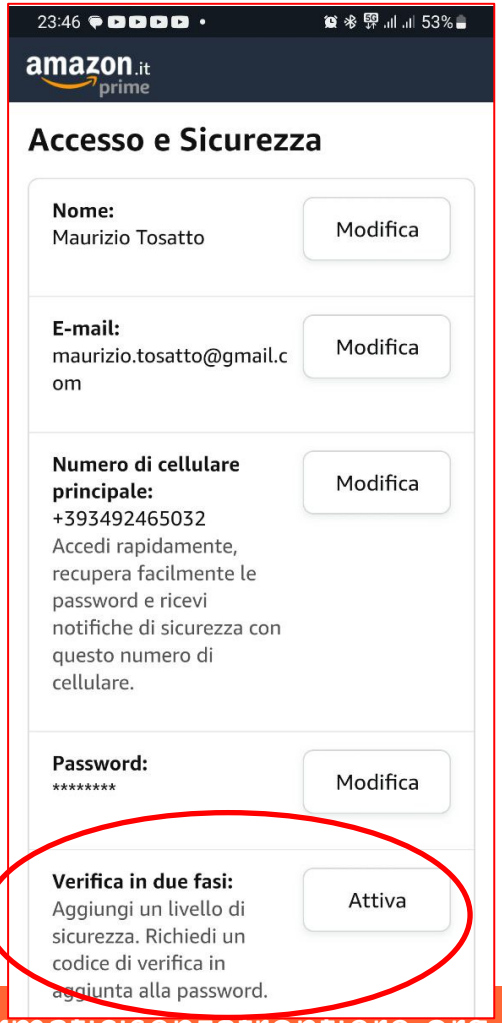




Esempio di autenticazione a due fattori: l'account Amazon

Come attivare l'autenticazione a due fattori

- In genere si accede dalla pagina delle "***Impostazioni di Sicurezza***" per attivarla.
- Viene chiesto come ricevere un codice di attivazione usa e getta, di solito tramite una mail o un SMS.
- Il metodo più sicuro è attraverso un **SMS**, quindi nella registrazione al sito dovremo indicare il nostro numero di telefono al quale ci verrà inviato il codice di attivazione.
- In seguito, ogni qual volta cercheremo di accedere al quel sito dovremo eseguire la procedura di autenticazione che prevede l'invio di un SMS o di una email con un codice per accedere al sito.



Esempio di autenticazione a due fattori: SPID

INFORMATICI SENZA FRONTIERE

AGID ITALIANO

SPID Sistema Pubblico di Identità Digitale

Seguici su Cerca

Cittadini Aziende Pubbliche Amministrazioni Cos'è SPID

Home / Cittadini

Attiva SPID

Se hai compiuto 18 anni e possiedi un documento italiano in corso di validità, puoi sbrigare la tua prossima pratica amministrativa **direttamente dal tuo smartphone, tablet o dal pc di casa.**

Come attivare SPID | Dove utilizzare SPID

Semplice

Prenotazioni sanitarie, iscrizioni scolastiche, servizi comunali, con un'unica credenziale (username e password).

Sicuro

L'accesso ai servizi è protetto, anche grazie a verifiche di sicurezza fino a tre livelli.
I tuoi dati non sono profilati e la tua privacy è garantita.

Veloce

Accedi ai servizi online ovunque ti trovi e da qualsiasi dispositivo.

Esempio di autenticazione a due fattori: CIE

INFORMATICI SENZA FRONTIERE

* La CIE3 è dotata di un microchip che contiene in un formato digitale sicuro tutti i dati personali, la foto e le impronte, è leggibile da Smartphone tramite il protocollo NFC

* Presenta notevoli caratteristiche anticontraffazione anche a livello visivo.

* Come per lo SPID consente l'accesso ai siti della pubblica amministrazione tramite l'App CieID (o tramite PC + lettore)

Sicurezza digitale: conclusioni

La sicurezza digitale:

- Non è un prodotto ma un processo con alcune **importanti regole** di prudenza da seguire
- La **tecnologia è sicura**, l'elemento più debole del sistema è la persona
- Non è un concetto assoluto, dipende dal contesto

La PRIVACY: meno si sa di me, meglio mi difendo!

INFORMATICI SENZA FRONTIERE

Il termine inglese **privacy** indica la **sfera privata degli individui**, e quindi fa riferimento all'insieme di informazioni personali, in particolari i **"dati sensibili"** (razza, orientamento sessuale, politico e religioso…) che vogliamo tenere riservati, abbiamo il:

- **diritto alla riservatezza**
- **diritto di scelta** sull'uso dei nostri dati

Privacy: cosa sono i cookie?

INFORMATICI SENZA FRONTIERE

- Ogni volta che visitiamo un sito web questo lascia innumerevoli tracce sul nostro browser e, più in generale sul nostro pc.
- Tecnicamente siamo noi che, collegandoci ad un sito internet gli chiediamo di inviarci tutte le sue componenti come immagini, testi, grafica, menù ecc.
- Vengono inviati anche dei file che raccolgono informazioni sull'attività dell'utente: i **cookie**, il cui scopo in origine era migliorare le funzionalità del sito.

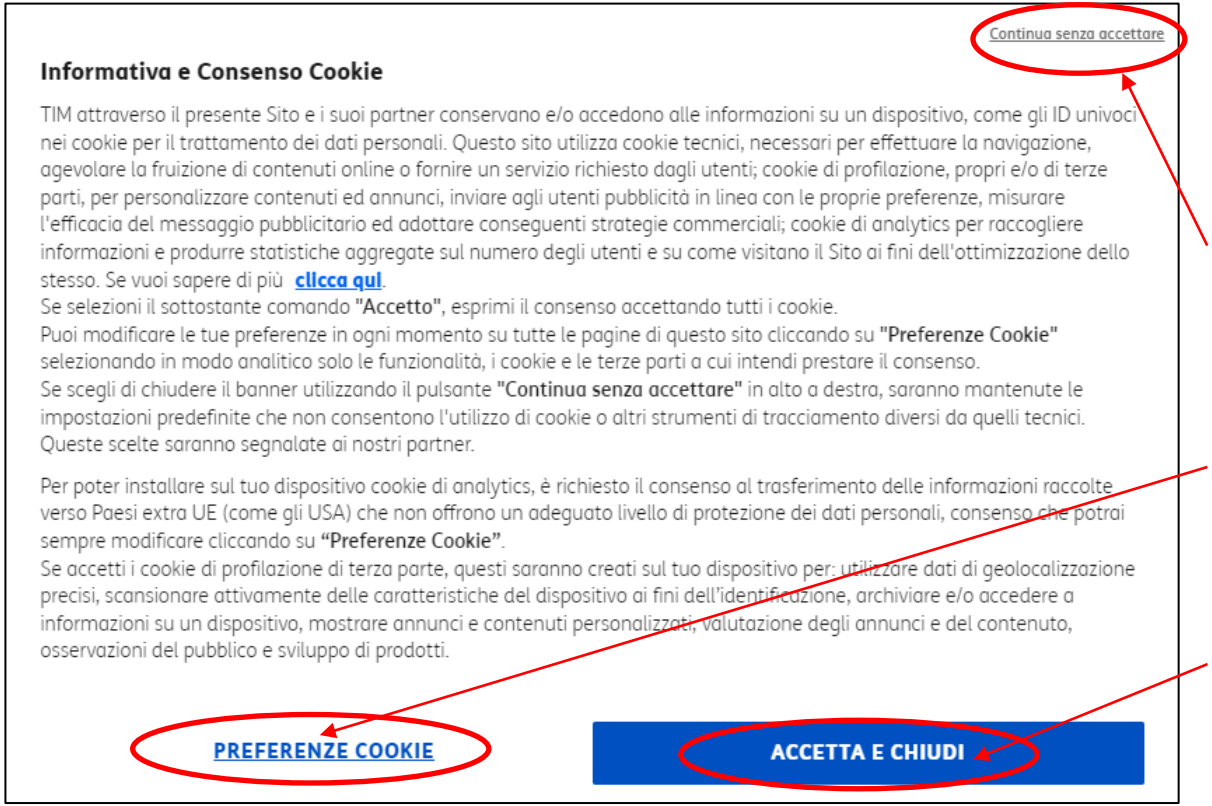
I cookie: tipologie

INFORMATICI SENZA FRONTIERE

- I cookie **tecnici:** permettono al sito di funzionare correttamente, consentendo al visitatore una migliore navigazione del sito, più veloce.
- I cookie **analitici** consentono al gestore del sito di raccogliere dati statistici: quanti visitatori, le pagine più lette, eccetera.
- Cookie di **profilazione**: sono solo questi quelli commerciali, che consentono l'invio di messaggi pubblicitari creati su misura in base ai gusti e alle preferenze manifestate in rete dall'utente profilato, con il rischio di venire indotti ad acquisti non preventivati.
- In genere solo per questi ultimi la norma richiede l'espresso consenso dell'utente; per i primi due il consenso è necessario solo se i cookie sono di terze parti e non resi anonimi.

I cookie: esempio di informativa e consenso

INFORMATICI SENZA FRONTIERE



Questa è una tipica finestra per la gestione del consenso sui cookie

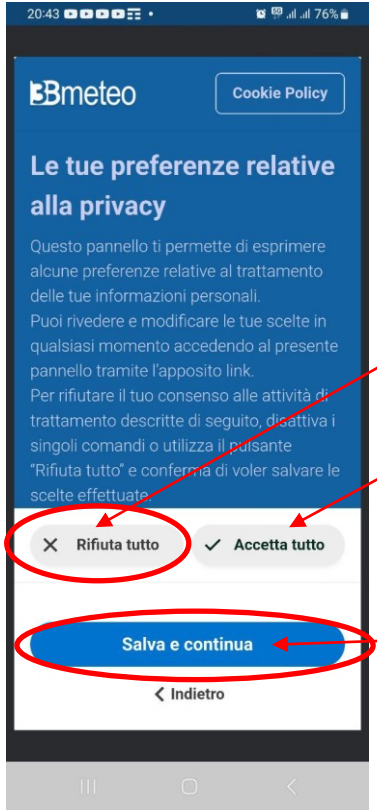
Continua senza accettare permette l'installazione dei soli cookie tecnici, sempre attivi. A volte c'è solo una X

Con **preferenze cookie** si possono selezionare le tipologie di cookie, difficile scelta per chi non ha un'adeguata competenza

Accetta e chiudi permette l'installazione dei tutti i cookie, inclusi quelli di profilazione di terze parti, quelli più "pericolosi" per la privacy

Il browser ricorda la scelta fatta e il consenso non viene più chiesto.

I cookie: esempio di informativa e consenso



Questa è una tipica finestra per la gestione del consenso per i cookie in uno smartphone

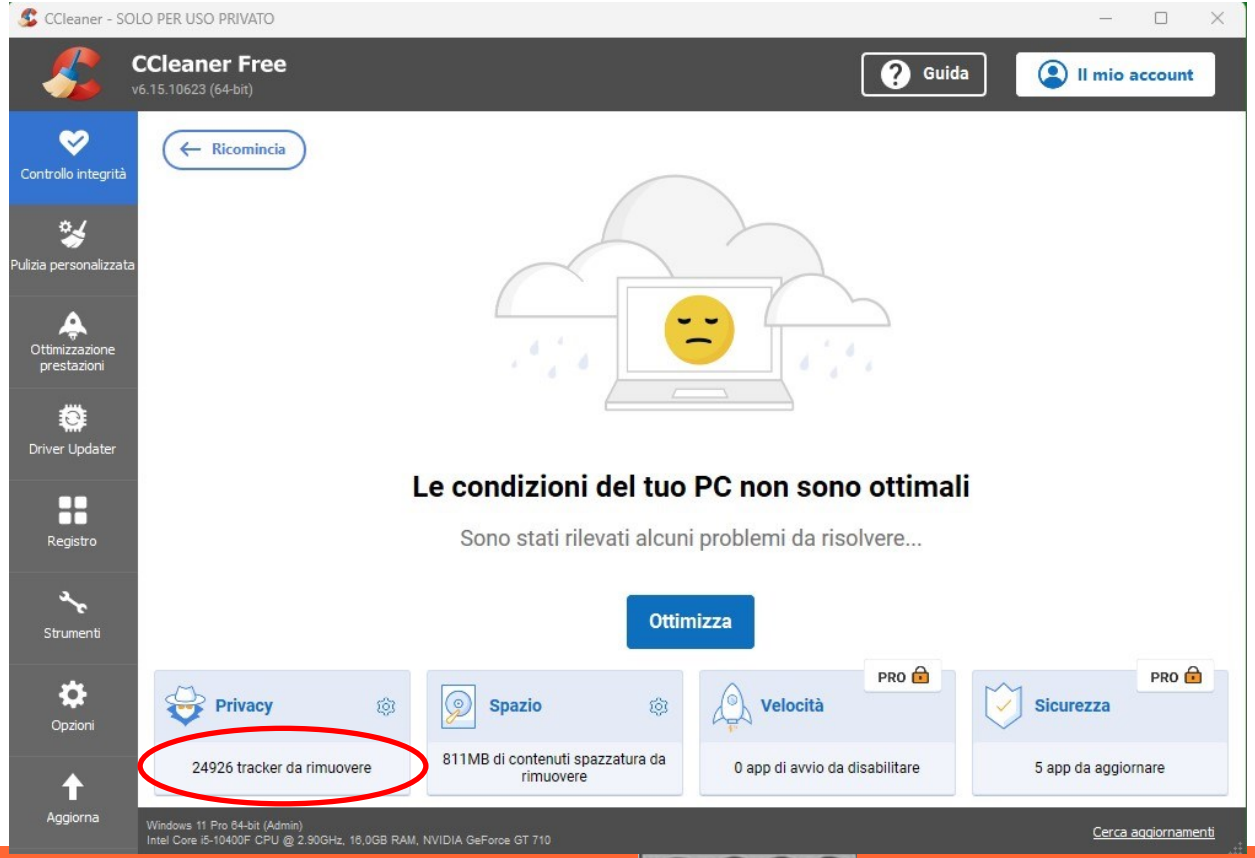
Rifiuta tutto permette l'installazione dei soli cookie tecnici, sempre attivi

Accetta tutto permette l'installazione dei tutti i cookie, inclusi quelli di profilazione di terze parti, quelli più "pericolosi" per la privacy

Fatta la mia scelta tocco salva e continua

I cookie: eliminarli con Ccleaner sul PC

INFORMATICI SENZA FRONTIERE



I cookie si possono eliminare nelle impostazioni del browser (Chrome, Firefox, Edge..)

Ccleaner (ed altri sw simili) permette di eseguire automaticamente la pulizia dei cookie per tutti i browser installati nel PC.

C'è anche per smartphone ma costringe a subire molta pubblicità…

Fake news, come scoprirle facendoci qualche semplice domanda:

INFORMATICI SENZA FRONTIERE

1. Chi ha pubblicato la notizia? (autore)
2. Si capisce qual è il suo lavoro e il suo titolo di studio?
3. Si può ritenere un esperto per l'argomento trattato?
4. A chi può far comodo o avere vantaggi dalla notizia?
5. Ci sono informazioni per contattarlo?
6. Vengono citate le fonti in modo verificabile?
7. Perché ci stiamo fidando e ci persuade questa persona? (Cercare risposte attendibili e non conferme!)
8. C'è una data di pubblicazione o aggiornamento?
9. Abbiamo verificato altre fonti?

Fake news = notizia falsa
Hoax = bufala
Fact checking = verifica dei fatti
Debunking = sfatare

INFORMATICI SENZA FRONTIERE

Cercare risposte attendibili e non conferme! Siti di verifica:

1. www.bufale.net BUFALE.NET
2. https://www.butac.it/ BUTAC
3. www.snopes.com (in inglese) Snopes
4. https://bufalopedia.blogspot.com/ (Paolo Attivissimo)

Motori di ricerca, come funzionano?

INFORMATICI SENZA FRONTIERE

- Scansionano continuamente il WEB per creare enormi cataloghi di pagine/contenuti e avere a subito a disposizione le informazioni cercate dall'utente, si possono dividere in:
  - Motori di ricerca commerciali (Google, Bing, Yahoo…), si paga per avere un posto prioritario nella lista dei risultati (sponsor)
  - Motori di ricerca orientati alla sicurezza/privacy dell'utente (Qwant, DuckDuckGo, Startpage…)
- Spesso usano le scelte degli utilizzatori stessi per ordinare la lista dei risultati.
- La presentazione dei risultati della ricerca può essere viziata da interessi economici o di opportunità politica

Grazie per l'attenzione!

maurizio.tosatto@informaticisenzafrontiere.org

https://www.facebook.com/InformaticiSenzaFrontiere
https://twitter.com/informatici
https://www.linkedin.com/company/informatici-senza-frontiere-onlus
https://www.youtube.com/user/ISFItalia
https://www.instagram.com/explore/tags/informaticisenzafrontiere/