Truffe e raggiri in rete

Sicurezza digitale e tutela della privacy

Padova, settembre/ottobre 2023

Truffe, un allarme sociale!!!!

INFORMATICI SENZA FRONTIERE

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

INFORMATICI SENZA FRONTIERE

- 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

La Polizia ha la necessità di avere informazioni sui tentativi di truffa per poter individuare persone pericolose.

È necessario denunciare le truffe subite e segnalare situazioni sospette

Truffe alla porta di casa

INFORMATICI SENZA FRONTIERE

Mai aprire la porta a chi dice che c'è un'emergenza, le perdite di acqua e di gas sono una scusa!

Mai far vedere la bolletta a sedicenti "tecnici"!!!
Contiene codici con cui sottoscrivere contratti a nostra insaputa

Truffe in strada: lo specchietto rotto

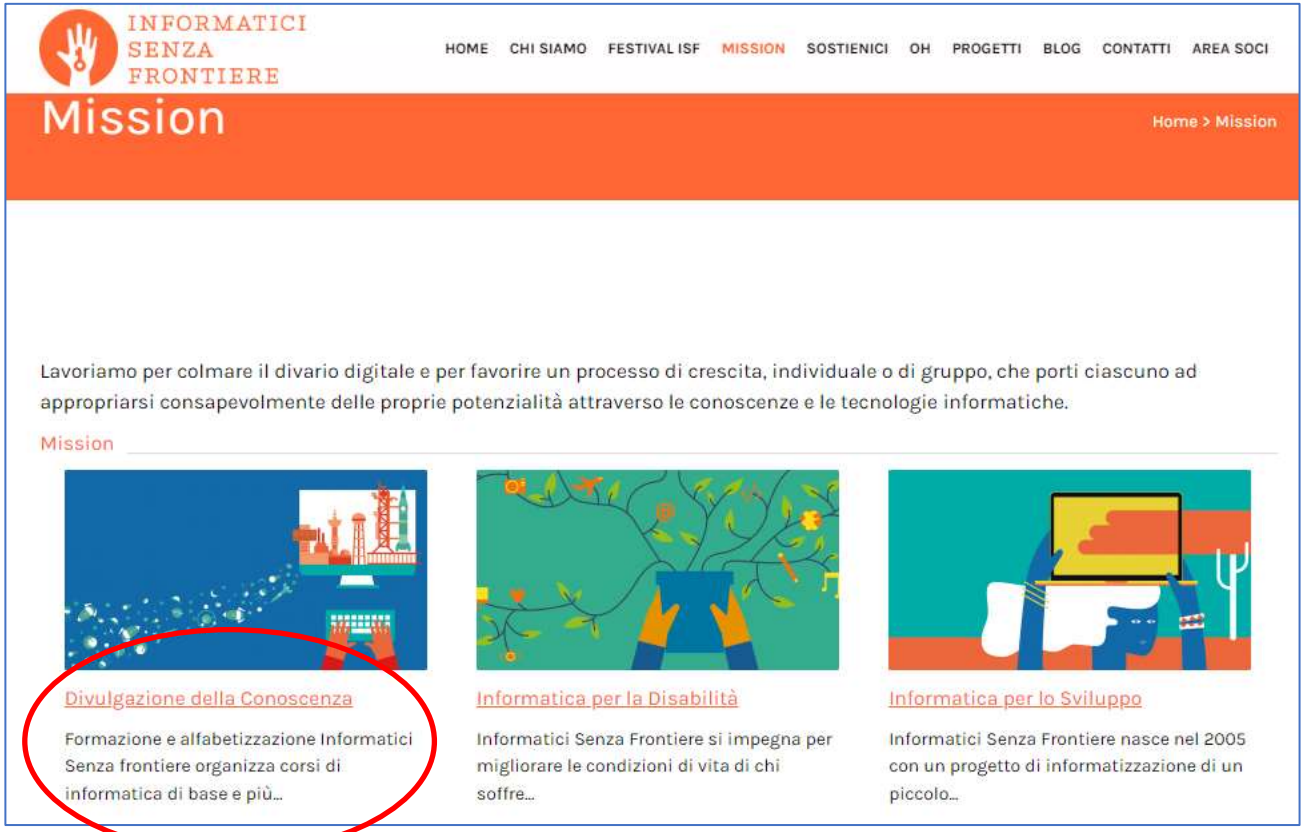
INFORMATICI SENZA FRONTIERE

- Mentre guidate per strada vi supera un auto che vi invita a fermarvi.
- Il guidatore, a volte una bella ragazza, vi segnala che passandogli accanto gli avete rotto lo specchietto.
- È molto comprensivo, non pretende che compiliate la constatazione amichevole (CAI, ex CID), si può sistemare tutto con una cifra in contanti di poche decine di euro… siate cortesi per non farvi aggredire.
- Ovviamente lo specchietto era già rotto! Viene simulata la rottura con il lancio di un sasso contro la vostra auto.
- Dite di aver dimenticato il portafoglio e chiedete di compilare la CAI e far intervenire carabinieri, polizia o vigili, di solito non insistono oltre.
- Ricordatevi di levare la chiave dal quadro e tenerla con voi e prendete nota della targa dell'auto.

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

Informatici senza Frontiere, chi siamo…



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.

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

INFORMATICI SENZA FRONTIERE

- 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

- **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)

INFORMATICI SENZA FRONTIERE

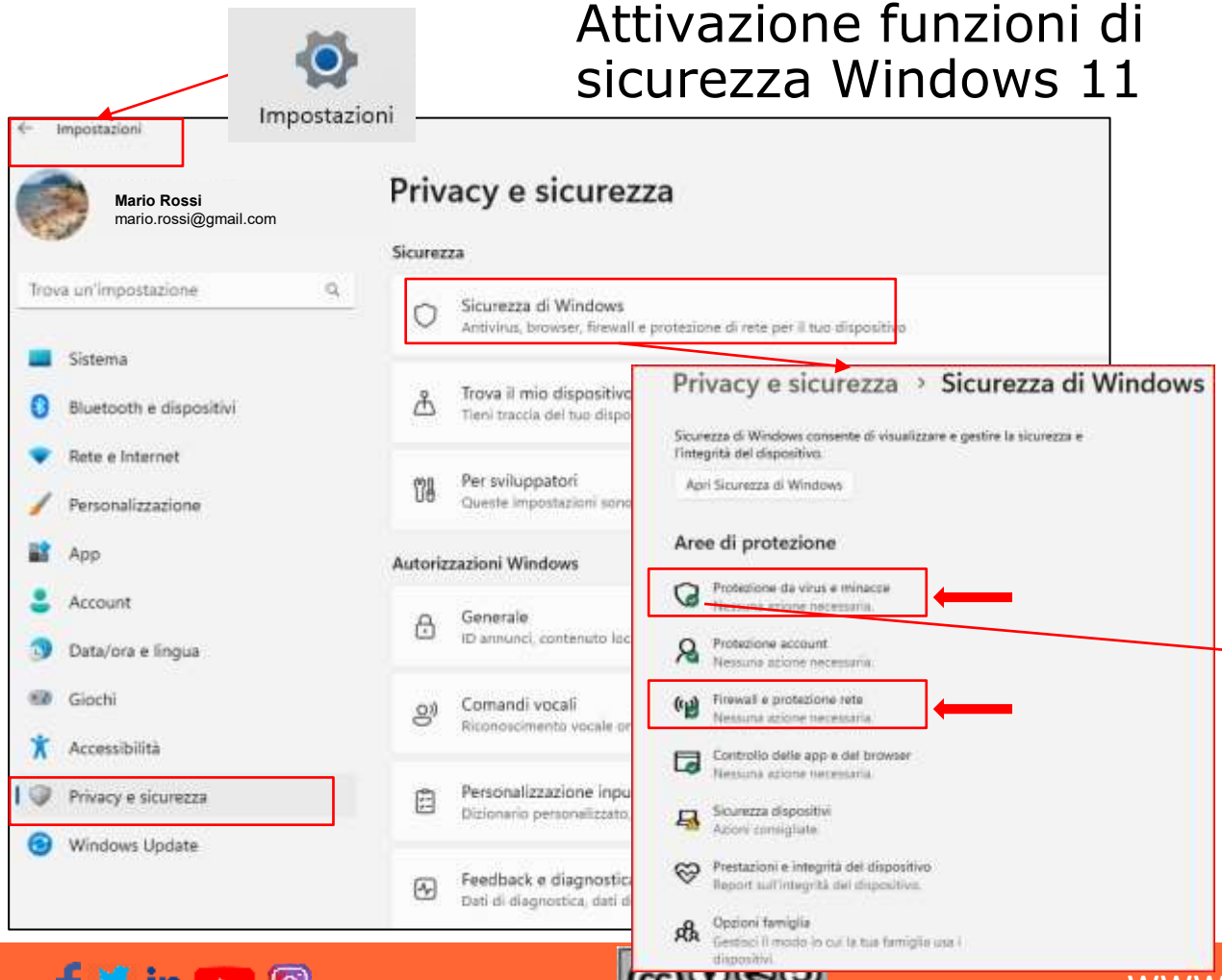
- Non inserite PIN/Password e dati personali su pc ad uso pubblico o connessi a reti pubbliche (WiFi al bar o in aeroporto) in particolare se aperte (no password)

- Valutate l'uso di una **VPN** (connessione criptata gratuita o a pagamento) che permette di non apparire direttamente in Internet

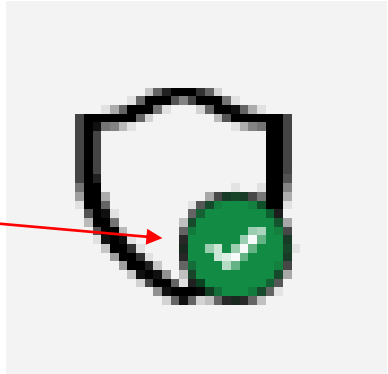
- Non cliccate sulle **finestre popup,** specialmente se avvertono della presenza di virus sul computer e offrono soluzioni, non selezionate il link e non autorizzate nessun download. Potreste scaricare e installare software dannosi

- Non usate versioni gratuite "craccate" di programmi a pagamento, potrebbero contenere virus, spyware, trojans... Oltretutto è un reato!

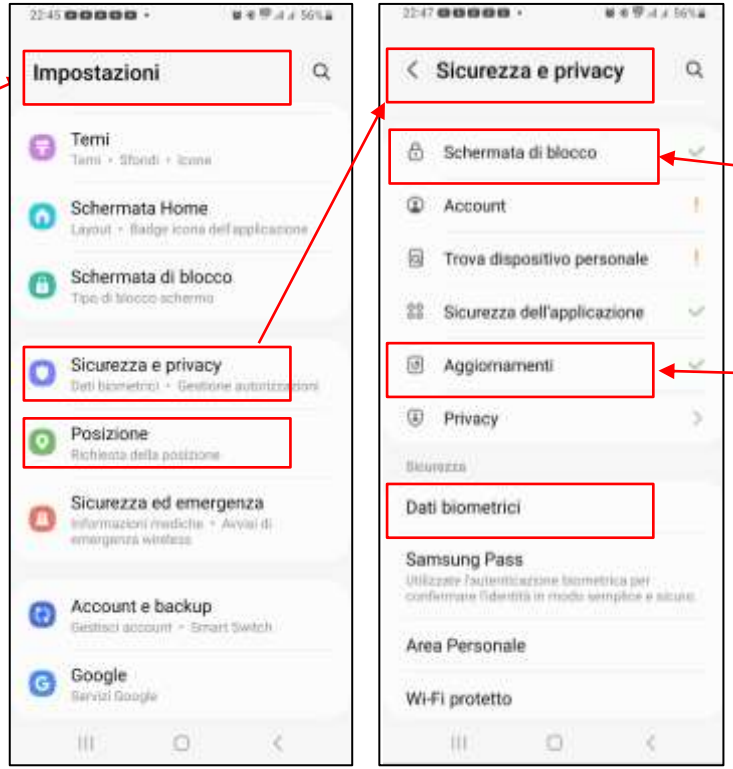
Attivazione funzioni di sicurezza Windows 11



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



Attivazione funzioni di sicurezza ANDROID



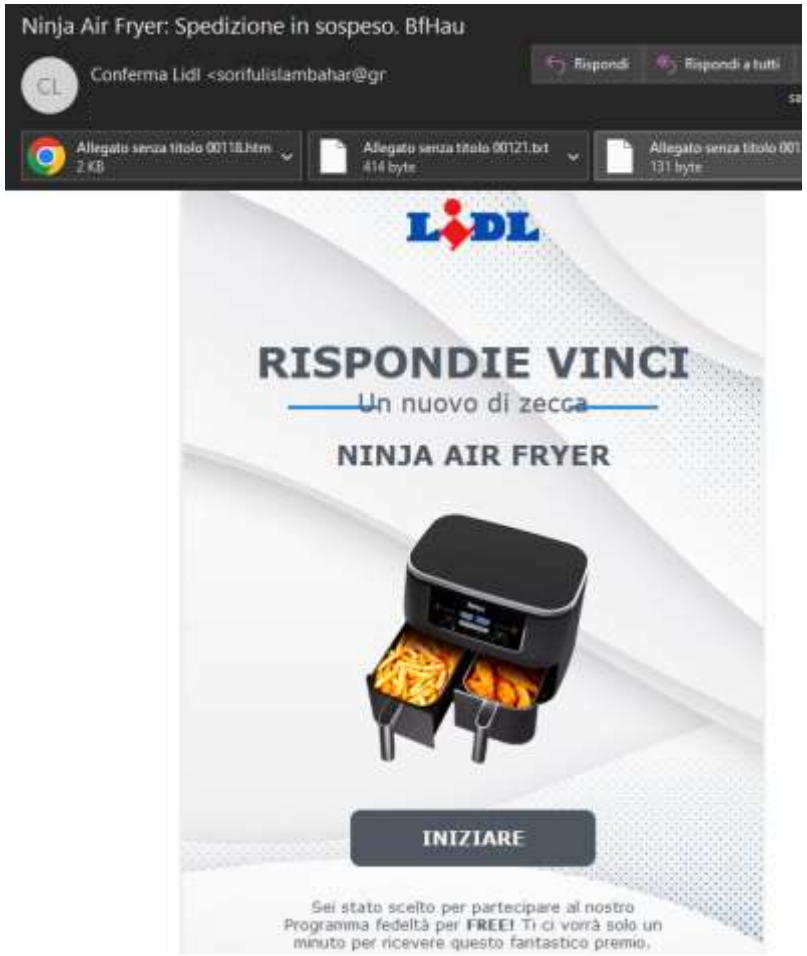
- Le funzioni di sicurezza standard sono sufficienti per il controllo del dispositivo
- Come per il PC è sempre bene avere almeno un **PIN per l'attivazione dello schermo**, indispensabile se lo si usa per i pagamenti
- E' opportuno personalizzare alcune funzioni come la possibilità di **aggiornamento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

Sicurezza digitale: Phishing e SMiShing

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

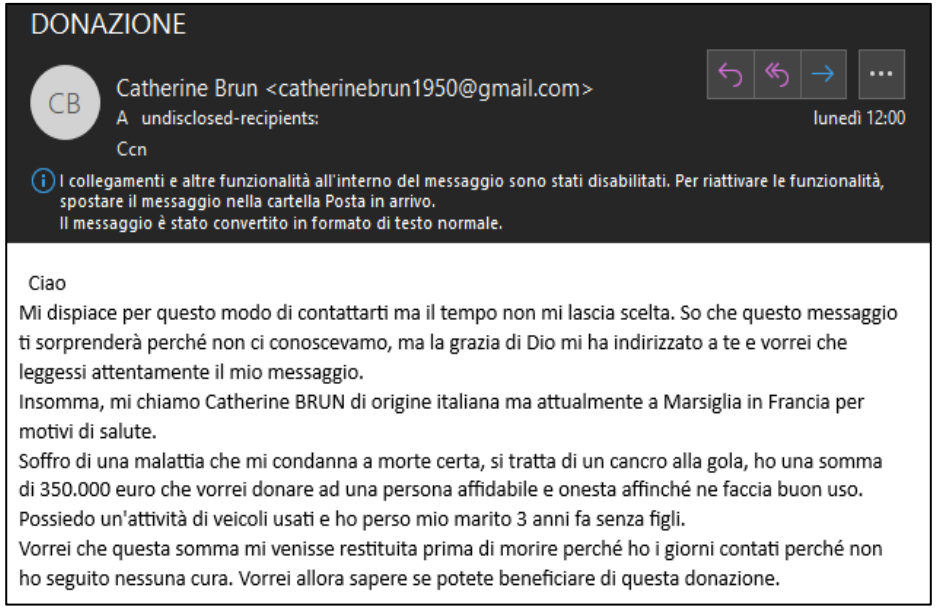


Esempio di email phishing che propone una vincita.

- 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.

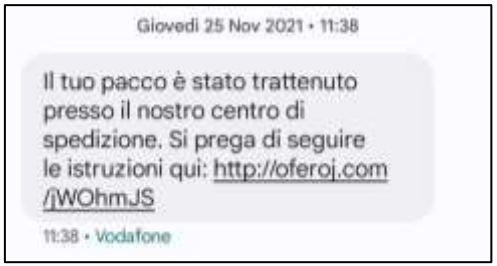
Esempio di email phishing che propone la donazione di una somma importante.

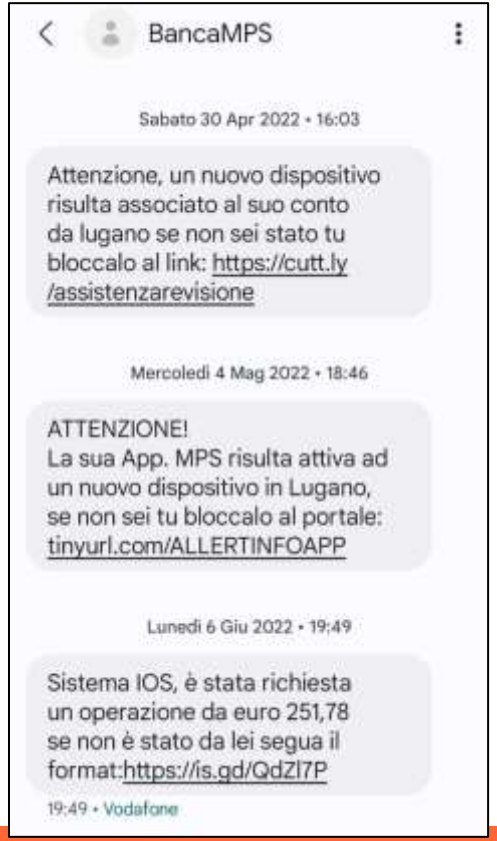
Cosa pensare?

- 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





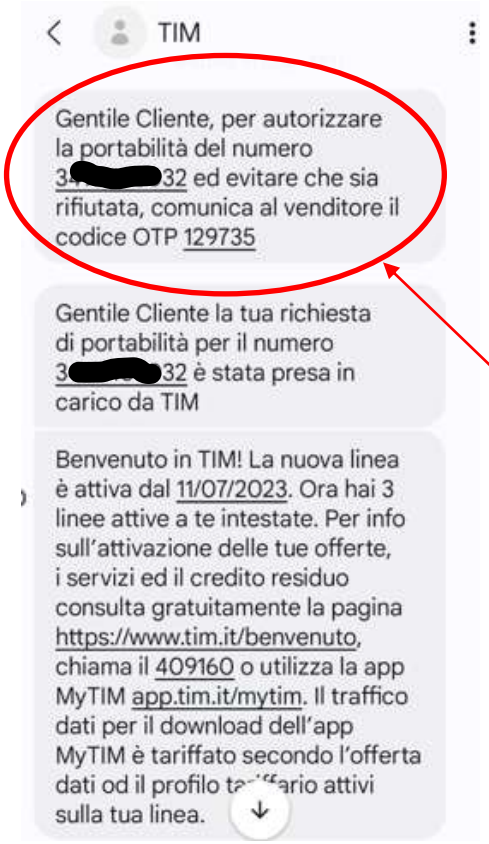
Esempi di SMS fraudolenti.

Simulano la 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: SIM swap



I messaggi SMS non sono da ignorare, sono ancora molto usati da chi non ha WhatsApp, per inviare i codici per l'accesso a 2 fattori e dalla Protezione Civile (IT-alert) in caso di necessità perché arrivano con certezza…

Una tipologia di messaggi SMS che deve essere attentamente considerata è quella inviata dai fornitori di servizi telefonici (es. TIM, VODAFONE, WIND…) per il cambio della SIM (SIM swap)

Dal 14.11.2022 è diventato obbligatorio inviare un messaggio SMS in tutti i casi in cui si procede alla sostituzione di una SIM. (AGICOM 86/21/CIR)

Questi messaggi contengono un codice che deve essere riferito all'operatore per poter procedere con la disattivazione della vecchia SIM e l'attivazione della nuova sullo stesso numero di telefono.

Nel caso in cui la vecchia SIM sia stata persa o rubata, non essendo possibile ricevere il messaggio SMS la procedura prevede comunque la disattivazione sulla base della denuncia all'autorità.

Se qualcuno sta cercando di **clonare il vostro telefono** con l'aiuto di un operatore compiacente o simulando perdita/furto è importante contattare subito l'operatore per informarlo che si sta subendo un **furto di identità**!!!!

Consigli per evitare Phishing e SMiShing

INFORMATICI SENZA FRONTIERE

- Non rispondete **mai** a messaggi o telefonate che chiedono informazioni bancarie/finanziarie, personali o documenti di identità.
- Se avete dubbi contattate gli enti coinvolti tramite **canali ufficiali**.
- Attenti a gestire e-mail e dati personali. Non rivelate a nessuno e non comunicate i codici o password e non inviateli mai tramite email
- Non aprite e non rispondete ai messaggi di posta indesiderata (**spam**)
- Non cliccate sui **link** presenti all'interno dei messaggi da mittente dubbio/sconosciuto o di posta **spam**. Possono indirizzarvi su un sito fittizio per carpire informazioni personali, come dettagli bancari e codici di accesso.

Sicurezza digitale: QRishing

- **Scansionare un codice QR** è rischioso perché equivale alla veloce **digitazione di un link**
- In genere si scansionano usando App specifiche che permetto di controllare il link prima di usarlo
- Si deve diffidare degli **short link** (link abbreviati) che non provengono da fonte certa dato che il link originale da cui provengono è sconosciuto.
- Meglio evitare la scansione di codici in posti dove chiunque potrebbe averli posizionati o modificati con etichette adesive

Mettiti alla prova!

INFORMATICI SENZA FRONTIERE

https://phishingquiz.withgoogle.com

Siti fasulli: assicurazioni RCA on-line

- 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)

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

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

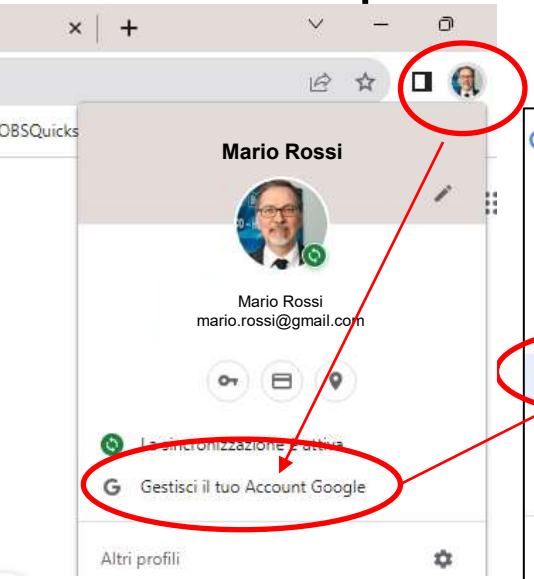
- Risolvono il problema di dover ricordare le password lunghe e complesse inserendole automaticamente.
- **Gratuiti**: KeePass, Bitwarden, Sophos Intercept X for Mobile
- **A pagamento**: LastPass, 1Password, Dashlane, Keeper
- **Integrati nel browser**: Safari, Google Chrome, Mozilla Firefox, Microsoft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

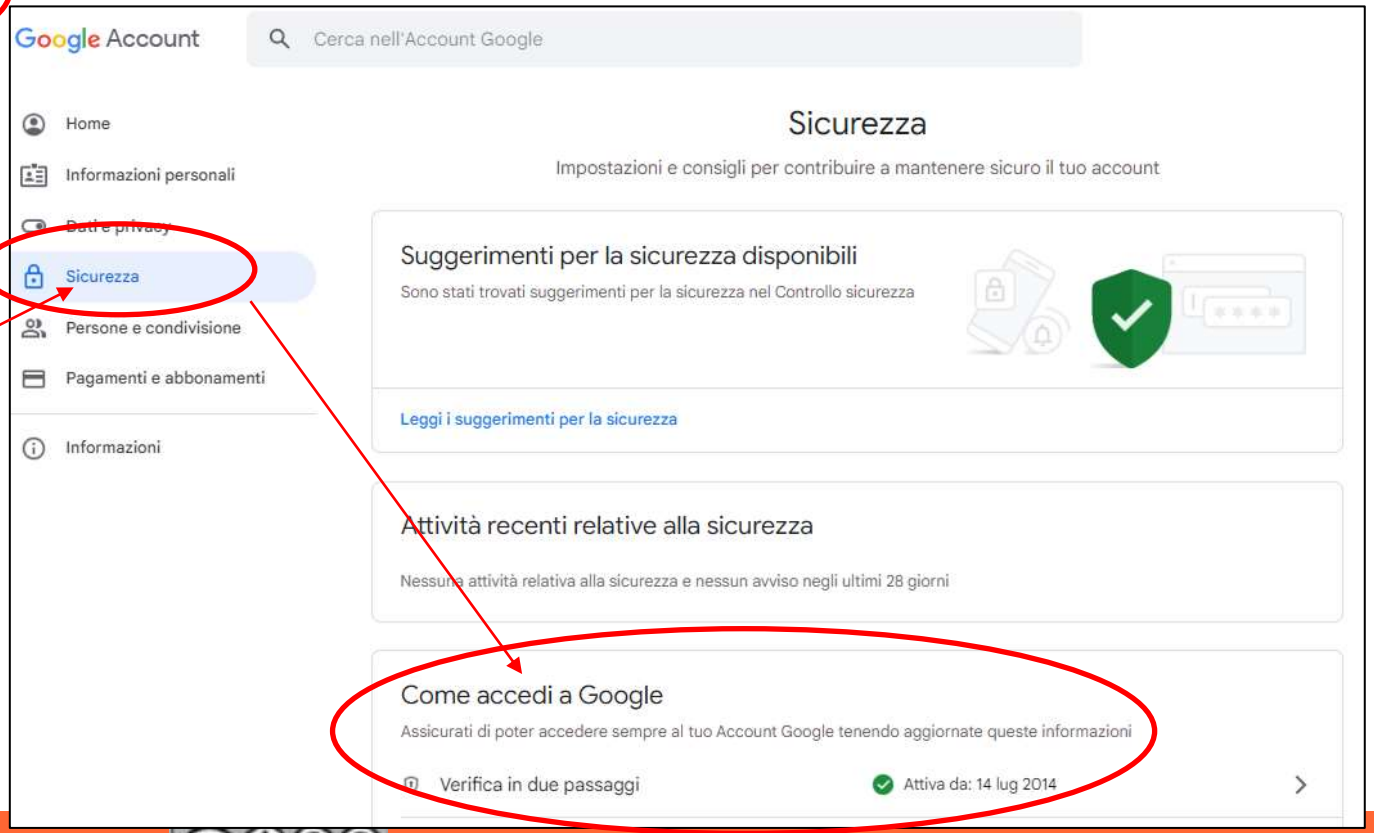
L’autenticazione a due fattori (2FA)

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 col codice da riportare sul 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

* 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)

Cos'è il sistema di comunicazione NFC ?

INFORMATICI SENZA FRONTIERE

- NFC è una comunicazione radio molto usata, per esempio nei sistemi di pagamento "contactless": carte di credito, bancomat e negli e-wallet degli smartphone (Google Pay, ApplePay)
- La caratteristica più interessante è che uno dei due dispositivi può non avere la batteria, questo ha permesso la realizzazione delle "smart card" contactless come CIE, carte di credito, bancomat ecc.
- Può trasmettere al massimo fino a pochi mm, la custodia del telefono può creare problemi
- È ormai disponibile in quasi tutti i moderni Smartphone anche di basso costo ma deve essere attivato nelle impostazioni allo stesso modo di WiFi o Bluetooth
- Per impedire la lettura della carta (molto improbabile) esistono in commercio dei "portacarte schermati". Gli smartphone non hanno questo problema, a schermo spento non è possibile il pagamento.

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
- 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.

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

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

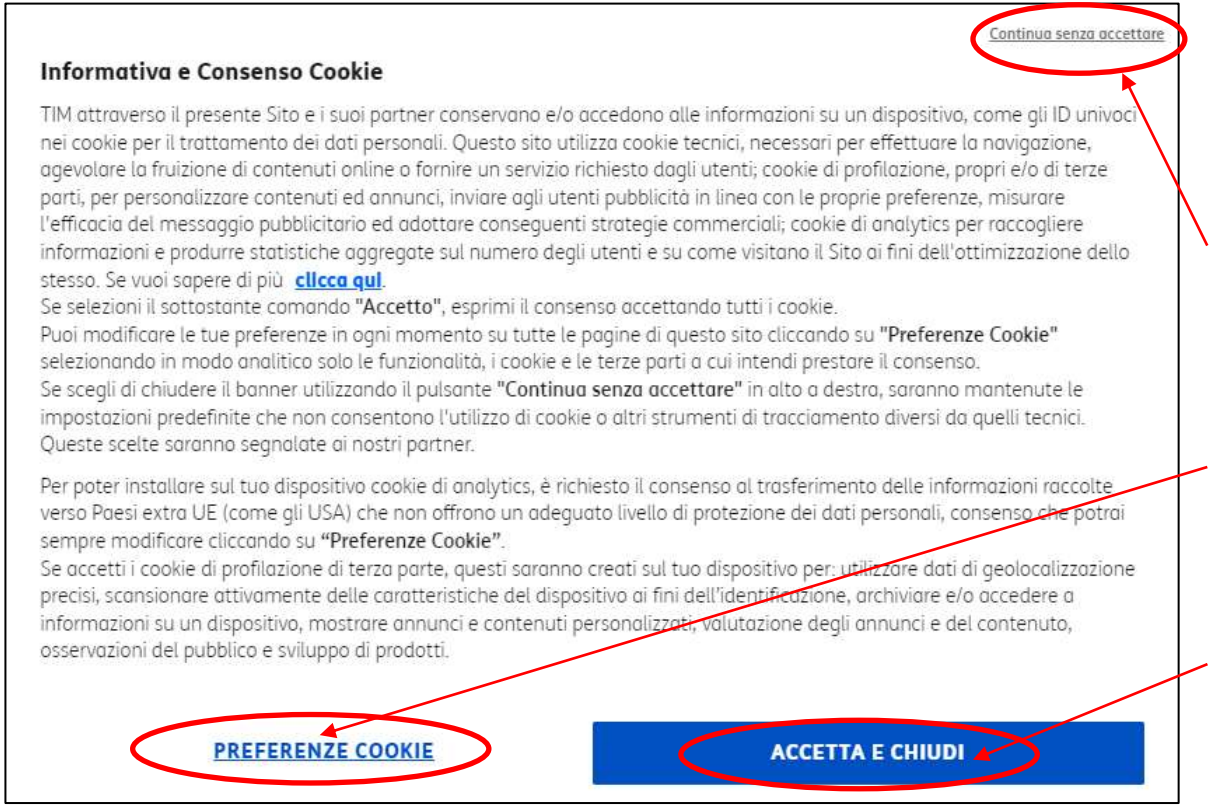
- Ogni volta che visitiamo un sito web questo lascia innumerevoli tracce sul nostro browser e, più in generale sul nostro pc.
- Tecnicamente siamo noi che, collegandoci ad un sito internet gli chiediamo di inviarci tutte le sue componenti come immagini, testi, grafica, menù ecc.
- Vengono inviati anche 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



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

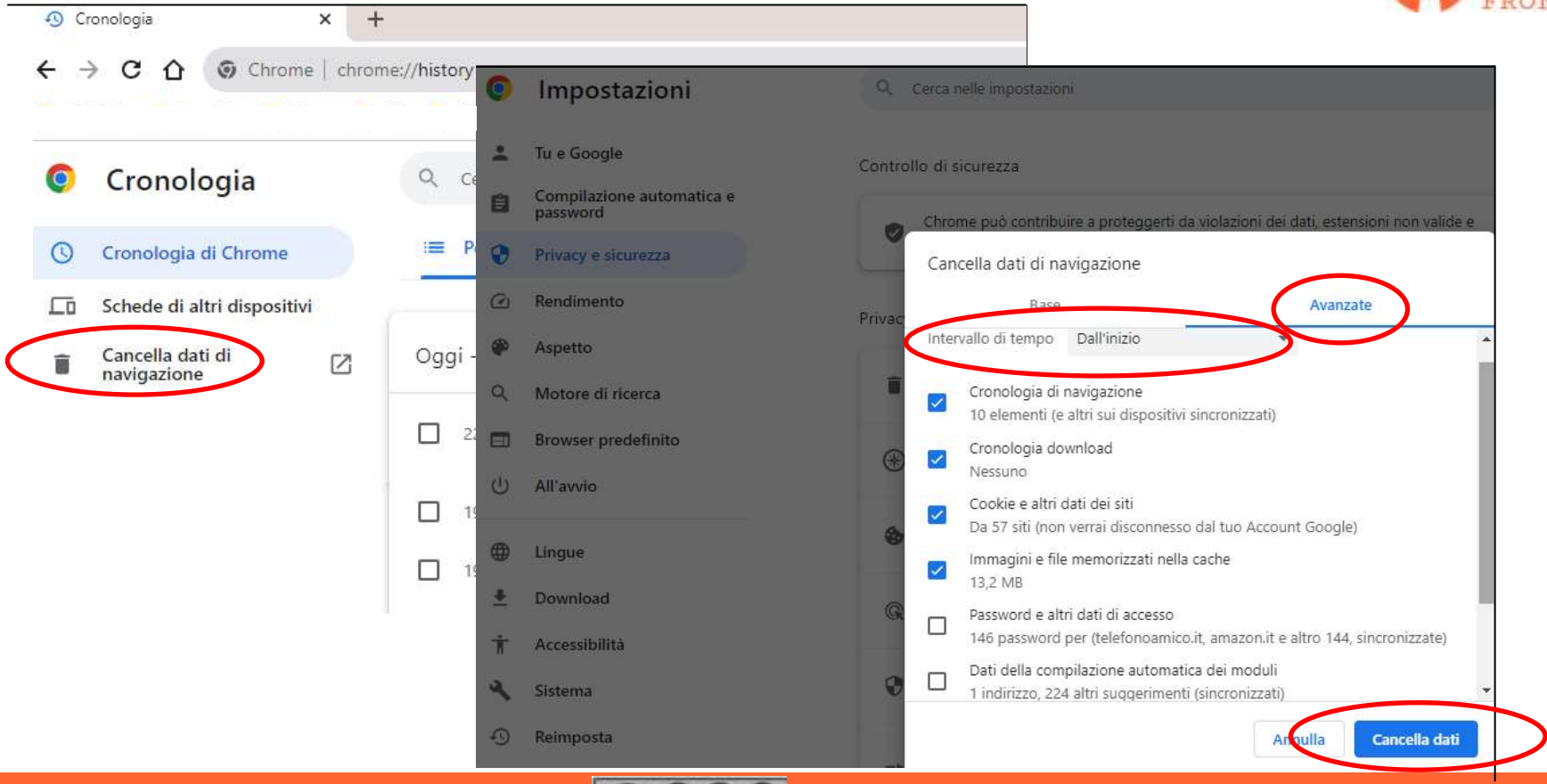
Rifiuta tutto permette l'installazione dei soli cookie tecnici, sempre attivi

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

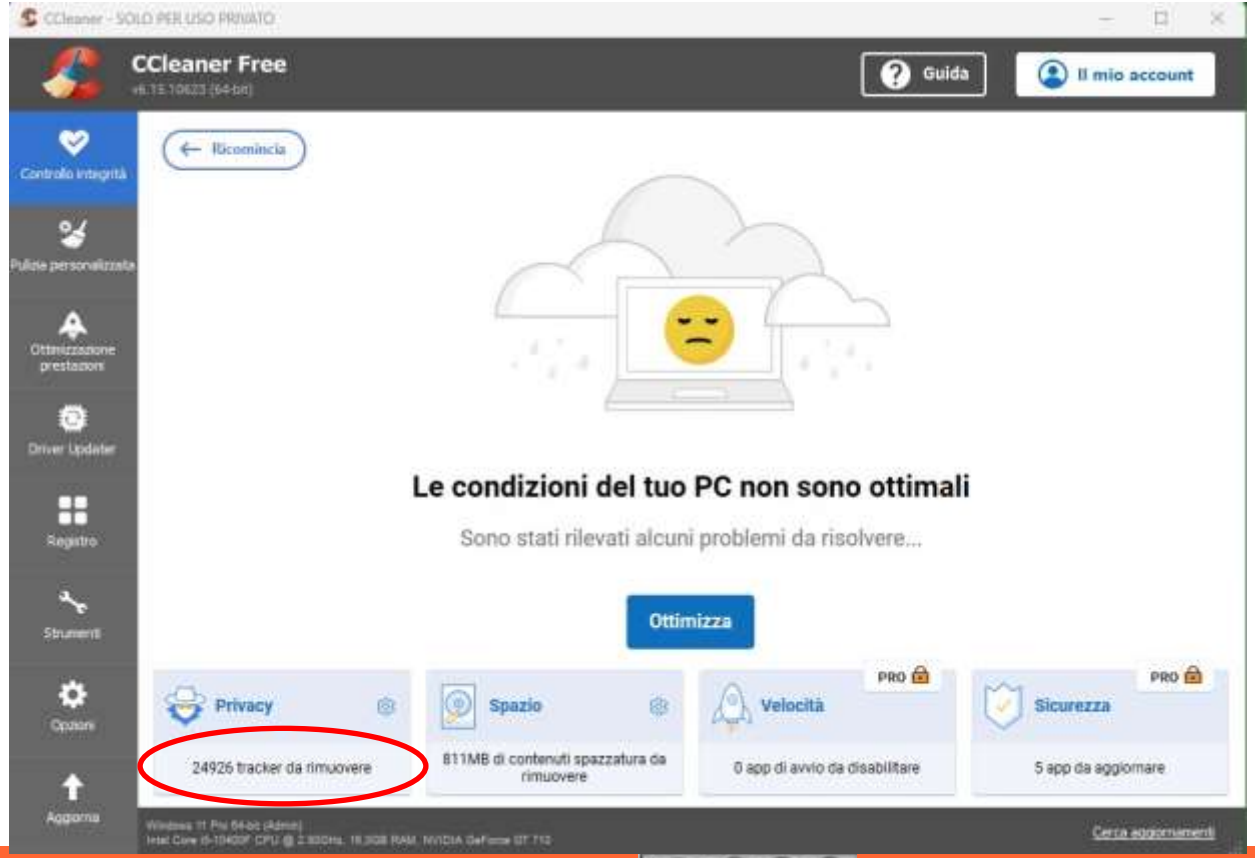
Fatta la mia scelta tocco salva e continua

I cookie: come eliminarli da Chrome

INFORMATICI SENZA FRONTIERE



I cookie: eliminarli con Ccleaner sul PC

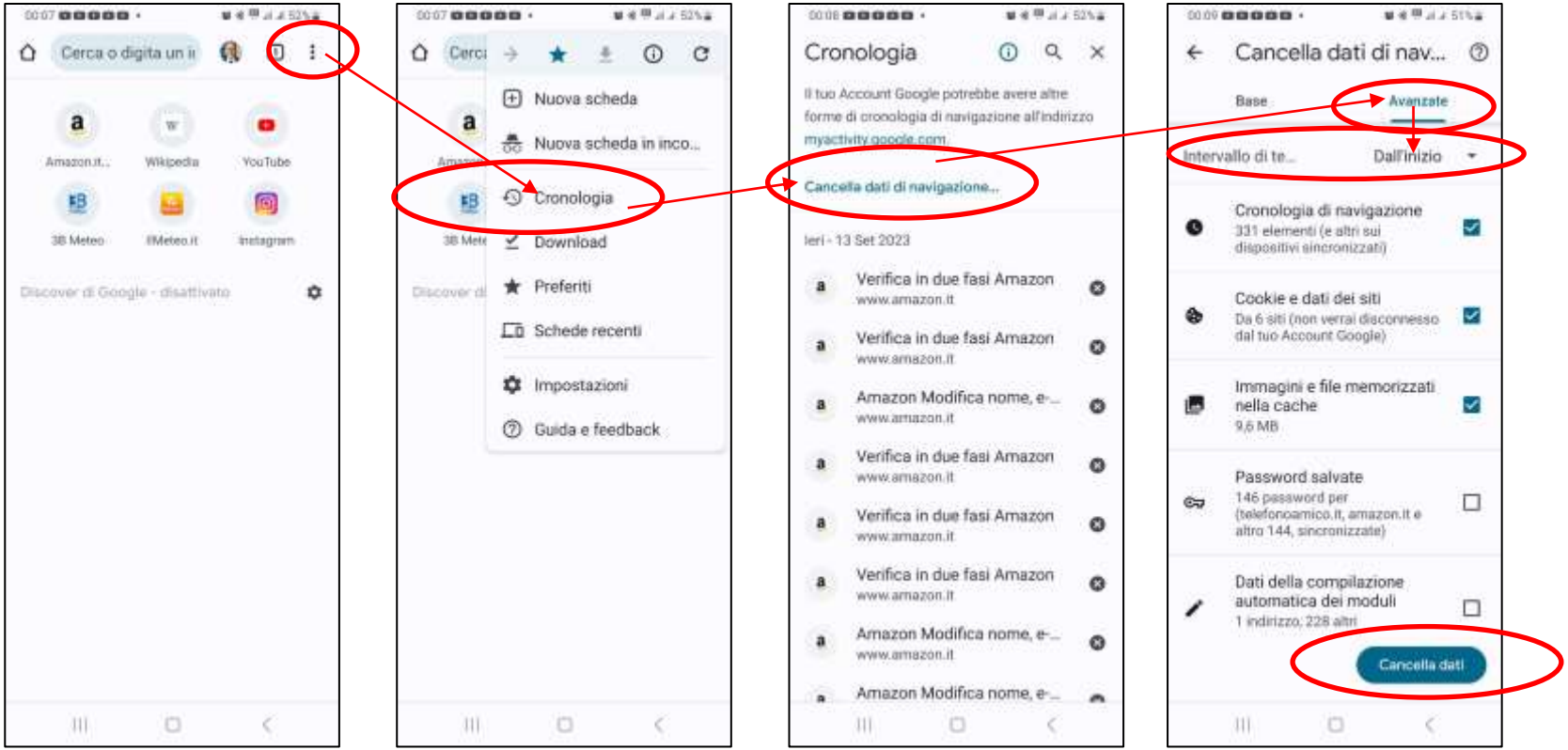


I cookie si possono eliminare nelle impostazioni del browser (Chrome, Firefox, Edge..)

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…

I cookie: eliminarli da Chrome su Android



Sicurezza digitale e tutela della privacy:

INFORMATICI SENZA FRONTIERE

1. usare password complesse e varie
2. usare programmi antivirus/antispyware
3. usare i social come se si fosse in pubblico
4. non pubblicare documenti di identità su social o chat pubbliche
5. non postare sui social foto/video di minori
6. evitare le reti WiFi pubbliche; in caso di necessità, usare la navigazione in incognito
7. accettate solo i cookie tecnici e quelli analitici di prima parte
8. controllare periodicamente le impostazioni di sicurezza dei vostri account

In caso di necessità...

- www.garanteprivacy.it

- https://www.commissariatodips.it/

- https://www.poliziadistato.it/

Per ricevere supporto puoi rivolgerti agli

SPORTELLI DI PROSSIMITÀ

- **presso Ufficio "Attività creative Terza Età"**
  via Giotto 34 - **049 8205088**
  lun, mer, ven 9:00-12:00; mar 15:00-16.30.
- **con ACCESSO SU PRENOTAZIONE**
  al numero unico **375 6641680**, presso

- **Quartiere1: sede Acli**
  via Vescovado 33
  mar, mer 9:30 - 12:30
- **Quartiere2**: sede Acli
  via Buonarroti 62
  mar 15:00 - 17:00
- **Quartiere3: sede UIL a "La Corte"**
  a cura di Ass. Pio X Pescarotto
  via Bajardi 5
  mer, ven 9.30 - 11.30
- **Quartiere3: Spazio Prisma**
  via Maroncelli 63
  mar 9.30 - 11.30
- **Quartiere5: Spazio Prisma**
  via Magenta, 4
  due lun al mese, 10:00 - 12:00

IN COLLABORAZIONE CON:
Consulte di Quartiere - Acli Padova
Anteas San Pio X Pescarotto O.d.V.
Sezione Provinciale ENS di Padova

INFORMATICI SENZA FRONTIERE

In caso di necessità...

Grazie per l'attenzione!

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/