Lo so! usare bene e in sicurezza Internet e APP

Comune di Modena

MODENA CITTÀ SICURA

Polizia Locale
COMUNE MODENA

make it modena PALESTRA DIGITALE + INNOVATION LAB

MODI
modalitàdifferenti

Iniziativa realizzata nell'ambito del progetto ***La prevenzione rende sicuri: azioni integrate per il contrasto di truffe e raggiri ai danni della popolazione anziana,*** finanziato dal Fondo Unico di Giustizia del Ministero degli Interni, dall'Ufficio Amministrativo, Legalità e sicurezze con la collaborazione della Palestra Digitale Makeit Modena del Comune di Modena.

Comune di Modena

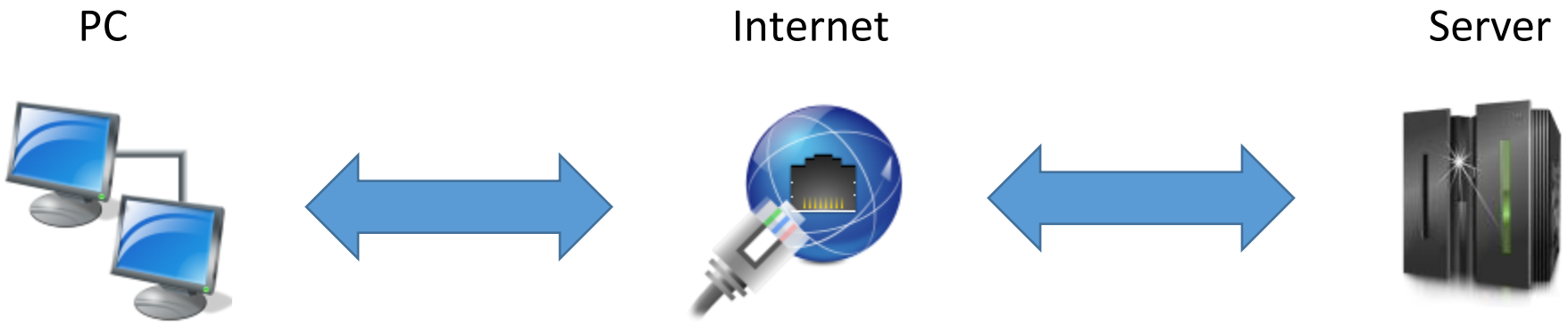
Modena città sicura

Polizia Locale

make it modena PALESTRA DIGITALE + FABLAB

Che cos'è Internet

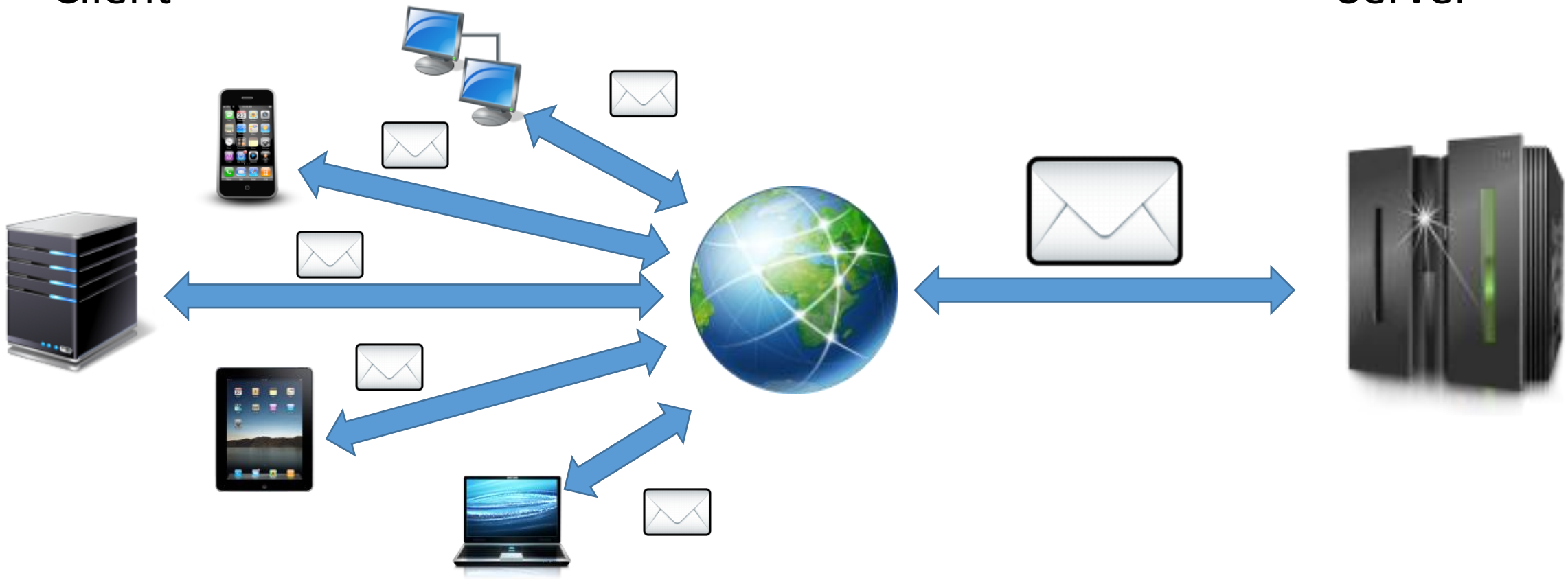
- Una rete di collegamenti informatici a livello planetario che permette la connessione e la comunicazione tra loro di reti locali di computer e banche dati, rendendone disponibili agli utenti le informazioni nella forma di immagini, filmati, ipertesti, musica; tra cui servizi di posta elettronica, web, social media.



Come funziona

- Client

Server



Word Wide Web (WWW)

- Tutti conosciamo il mondo di internet, con tutti quei siti di vari contenuti.
- Tutti i giorni ci navighiamo pensando che niente possa succedere, in questo mare di informazioni.
- Ecco il primo errore che facciamo, una buona parte degli attacchi informatici arriva proprio da internet. Essendo un mondo vasto bisogna far attenzione quando ci muoviamo, perché ogni sito potrebbe contenere un pericolo un virus.

Come si naviga ?

- Partiamo dando qualche consiglio di base come navigare:

1) Parole chiavi mirate nella ricerca, da scremare le informazioni.
2) Guardare estensioni pagina di internet, se ci avete fatto caso nei siti viene visualizzato URL. Esempio: www.wikipedia.com se notate qualcosa di strano vi consiglio di non cliccare il sito.
3) Attenzione al contenuto dei siti che scaricate, è molto importante quando eseguite un download, siate sicuri che il contenuto sia attendibile. Perché il pacchetto che scaricate potrebbe avere al suo interno un virus.
4) Nel caso non siete sicuri del sito, vi consiglio di chiedere a qualcuno più esperto di voi per essere tranquilli.

Google

1

wikipedia

Tutti Notizie Immagini Video Shopping Altro Impostazioni Strumenti

Circa 1.090.000.000 risultati (0,43 secondi)

2

it.wikipedia.org › wiki › Pagina_principale

Wikipedia, l'enciclopedia libera

Benvenuti su **Wikipedia** L'enciclopedia libera e collaborativa · Clicca qui per sfogliare l'indice delle voci! Sfoglia l'indice · Clicca qui per consultare il sommario ...

Wiki

Jimmy Wales - Disambigua - Wikimedia Foundation - ...

Lingua italiana

L'italiano ([ita'lja:no] ascolta) è una lingua romanza parlata ...

Altri risultati in wikipedia.org »

it.wikipedia.org › wiki › Wikipedia_in_italiano

Wikipedia in italiano - Wikipedia

Wikipedia in italiano è l'edizione in lingua italiana dell'enciclopedia online **Wikipedia**. Tale edizione, che ebbe inizio ufficialmente l'11 maggio 2001, è l'ottava ...

Tipo di sito: enciclopedia wiki
Stato attuale: attivo
Creato da: comunità italofona di Wikipedia
Proprietario: Wikimedia Foundation

www.wikipedia.org ▾ Traduci questa pagina

Wikipedia

Wikipedia is a free online encyclopedia, created and edited by volunteers around the world and

WIKIPEDIA
L'enciclopedia libera

Pagina principale
Ultime modifiche
Una voce a caso
Nelle vicinanze
Vetrina
Aiuto
Sportello informazioni

Comunità
Portale Comunità
Bar
Il Wikipediano
Fai una donazione
Contatti

Strumenti
Puntano qui
Modifiche correlate
Carica su Commons
Pagine speciali
Link permanente
Informazioni pagina
Elemento Wikidata

Stampa/esporta
Crea un libro
Scarica come PDF
Versione stampabile

In altri progetti

Pagina principale | Discussione | Leggi | Visua

3

Benvenuti su Wikipedia

L'enciclopedia libera e collaborativa

Sfoglia l'indice · Consulta il sommario · Naviga tra i portali tematici

Vetrina

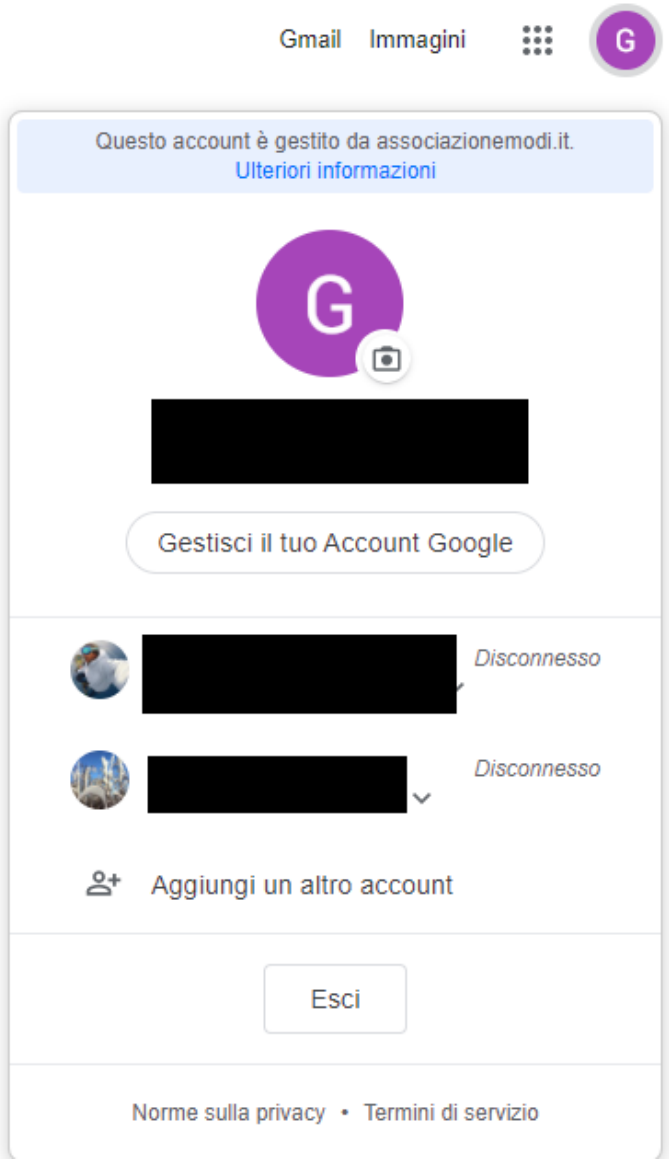
Pompei (in latino: *Pompeii*) è una città dell'evo antico, corrispondente all'attuale Pompei, la cui storia ha origine dal IX secolo a.C. per terminare nel 79, quando, a seguito dell'eruzione del Vesuvio, viene ricoperta sotto una coltre di ceneri e lapilli alta circa sei metri. Gli scavi della città, iniziati nel 1748, hanno riportato alla luce un sito archeologico entrato a far parte della lista dei patrimoni dell'umanità dell'UNESCO nel 1997, e che è il secondo monumento italiano per visite dopo il sistema museale del Colosseo, Foro Romano e Palatino.

Leggi la voce · Tutte le voci in vetrina

Voci di qualità

Cleomene III (in greco antico Κλεομένης, traslitterato in *Kleoménes*; Sparta, 260 a.C. circa – Alessandria d'Egitto, 219 a.C.) fu re di Sparta della dinastia agiade dal 235 a.C. al 222 a.C. Salì al trono nel 235 a.C. alla morte del padre Leonida II, che cinque anni prima aveva fatto giustiziare il collega re euripontide Agide IV e ne aveva fatto sposare la vedova Agiatide al figlio. Secondo la testimonianza di Plutarco fu Agiatide ad illustrare a Cleomene il progetto riformatore del suo primo marito, che proprio per questo era stato fatto uccidere da Leonida, e a convincerlo a seguire il progetto una volta salito al potere.

Il progetto di Agide consisteva in una riforma finanziaria che sanciva il condono totale dei debiti e in una riforma agraria che prevedeva la redistribuzione delle terre tra gli Spartani. L'intento era quello di riequilibrare così le ricchezze tra i cittadini in modo da

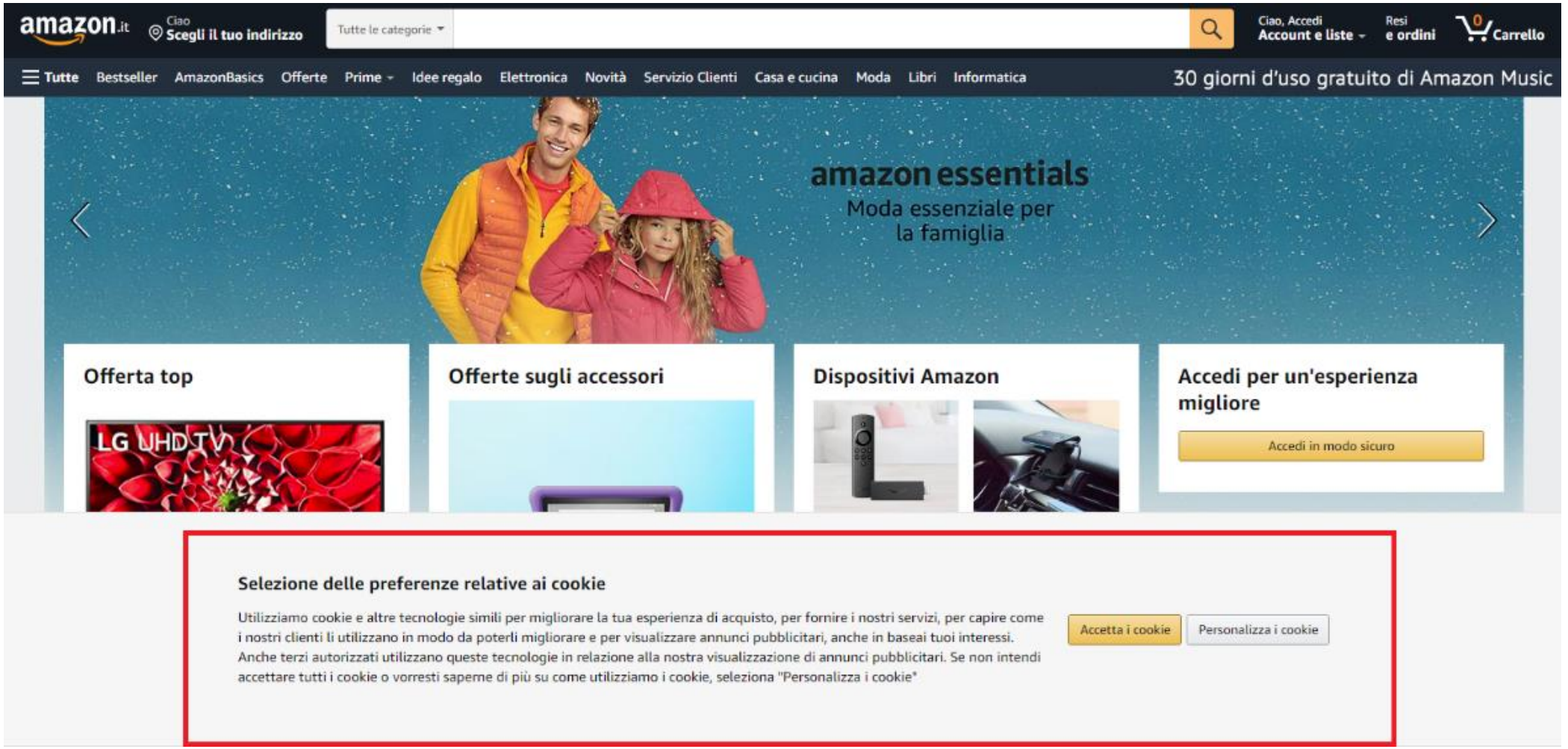


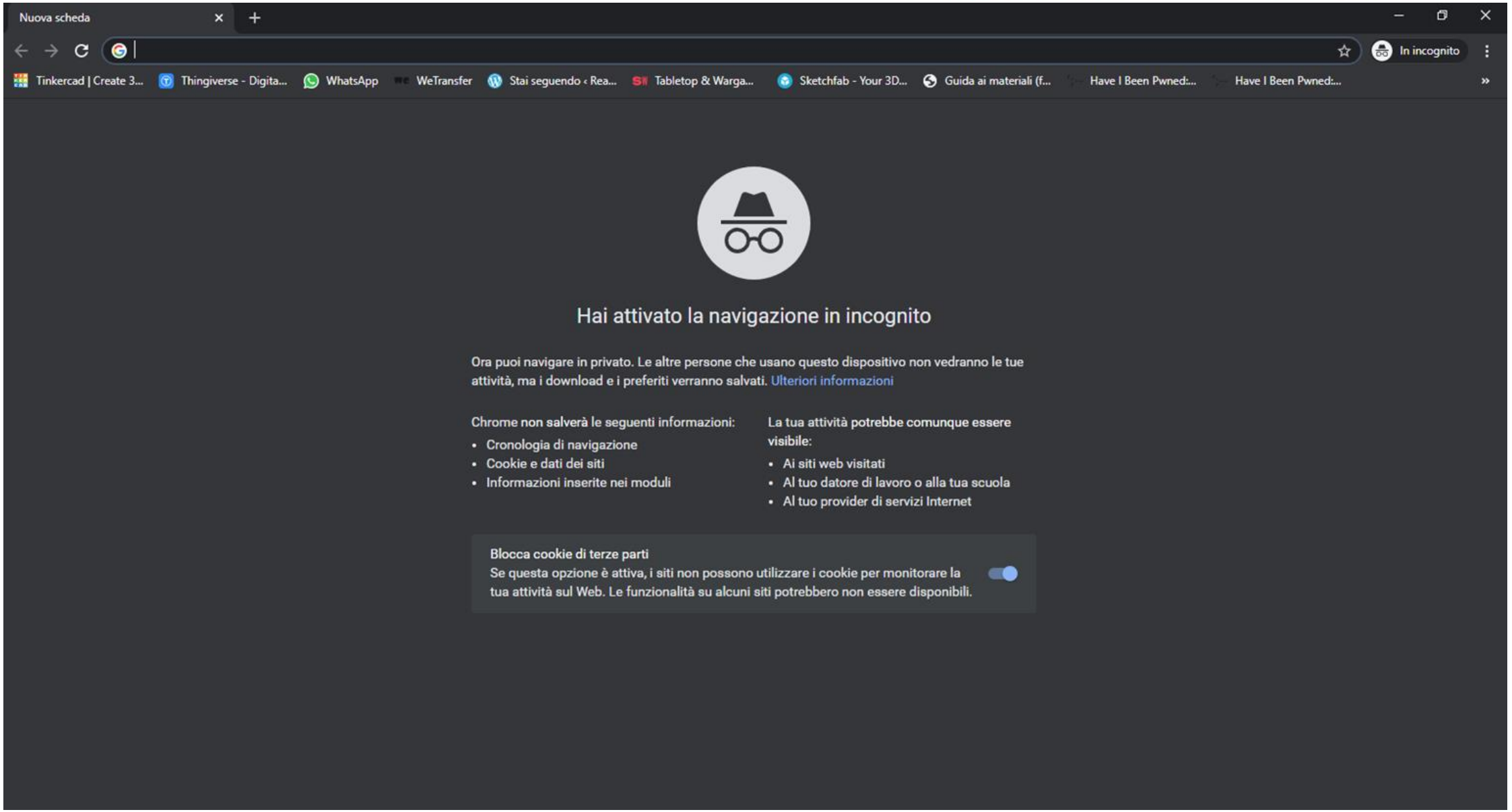
- Account browser e password,
- Molto importante non lasciare gli account collegati con i browser quando sono in costuditi.
- Perché? Possono leggere informazioni, cambiare la password, eseguire operazioni per conto vostro e molto altro.

- https://haveibeenpwned.com/

- https://haveibeenpwned.com/Passwords

Cookies


amazon.it
Ciao
Scegli il tuo indirizzo
Tutte le categorie
Ciao, Accedi
Account e liste
Resi
e ordini
0
Carrello
Tutte
Bestseller
AmazonBasics
Offerte
Prime
Idee regalo
Elettronica
Novità
Servizio Clienti
Casa e cucina
Moda
Libri
Informatica
30 giorni d'uso gratuito di Amazon Music
amazon essentials
Moda essenziale per la famiglia
Offerta top
LG UHD TV
Offerte sugli accessori
Dispositivi Amazon
Accedi per un'esperienza migliore
Accedi in modo sicuro
Selezione delle preferenze relative ai cookie
Utilizziamo cookie e altre tecnologie simili per migliorare la tua esperienza di acquisto, per fornire i nostri servizi, per capire come i nostri clienti li utilizzano in modo da poterli migliorare e per visualizzare annunci pubblicitari, anche in baseai tuoi interessi. Anche terzi autorizzati utilizzano queste tecnologie in relazione alla nostra visualizzazione di annunci pubblicitari. Se non intendi accettare tutti i cookie o vorresti saperne di più su come utilizziamo i cookie, seleziona "Personalizza i cookie"
Accetta i cookie
Personalizza i cookie


Nuova scheda
In incognito
Tinkercad | Create 3...
Thingiverse - Digita...
WhatsApp
WeTransfer
Stai seguendo ‹ Rea...
Tabletop & Warga...
Sketchfab - Your 3D...
Guida ai materiali (f...
Have I Been Pwned:...
Have I Been Pwned:...
Hai attivato la navigazione in incognito
Ora puoi navigare in privato. Le altre persone che usano questo dispositivo non vedranno le tue attività, ma i download e i preferiti verranno salvati. Ulteriori informazioni
Chrome non salverà le seguenti informazioni:
Cronologia di navigazione
Cookie e dati dei siti
Informazioni inserite nei moduli
La tua attività potrebbe comunque essere visibile:
Ai siti web visitati
Al tuo datore di lavoro o alla tua scuola
Al tuo provider di servizi Internet
Blocca cookie di terze parti
Se questa opzione è attiva, i siti non possono utilizzare i cookie per monitorare la tua attività sul Web. Le funzionalità su alcuni siti potrebbero non essere disponibili.

HACKERS
01
10
0101000
INFECTION
VIRUS
LOGIN
PASS
PROTECTION

Cosa sono i dati?

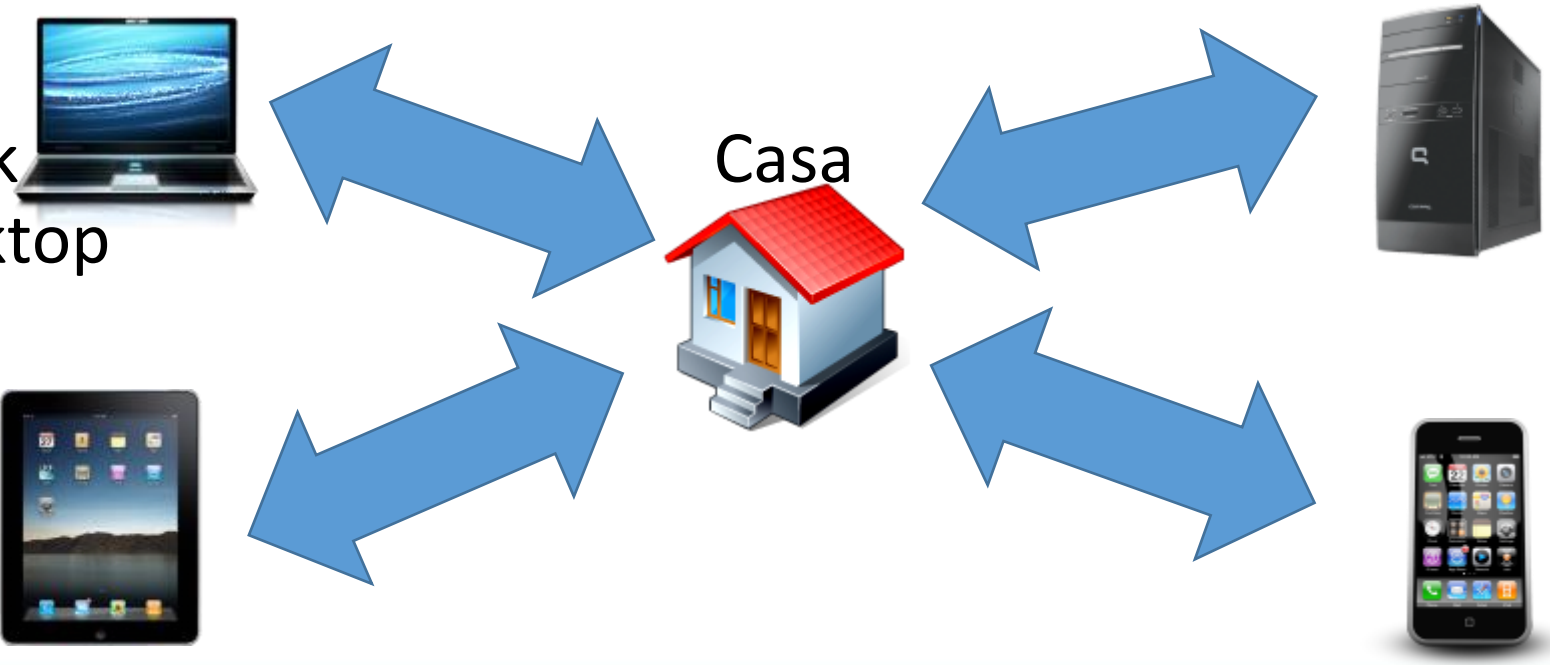
- I dati (File) sono delle informazioni digitali che contengono all'interno di un documento.
- Possono essere creati dal sistema operativo oppure dall'utente.
- Una volta generati i dati si possono leggere, scrivere, cancellare, visualizzarli, criptarli e molto altro.
- Quindi ogni documento che creammo al suo interno contiene informazioni per noi importanti.

Come mai i nostri dati sono cosi importanti ?

- Perché sono importanti, sia per noi che per hacker ?
- I dati contengono informazioni, da quelli più sensibili ad quelli meno sensibili.
- Ma gli hacker cosa se ne fanno di ogni singola informazione? Per loro è come una miniera d'oro.
- Il loro scopo e riuscire entrare nei vostri dispositivi di nascosto, per poi scaricare le informazioni da usare contro di voi oppure rivenderle al mercato nero Deep Web.
- Quindi cercano di intrufolarsi in ogni dispositivo, chiavette usb, hard disk esterni, credenziali siti, e molto altro.

Dati e Dispositivi

- Dove possiamo trovare i dati ?
- Molto semplice basti pensare ai dispositivi all'interno di una casa. Ognuno di loro genera dati di ogni tipo sia sensibili che del sistema per farli funzionare.



MALWARE PIÙ DIFFUSI

VIRUS

Produce sempre più **copie di sé** con cui infetta file o aree del disco. Richiede almeno un'interazione dell'utente.

TROJAN

Malware **mascherato** da software/file utile, che nasconde virus o elementi dannosi.

WORM

Malware **auto-replicante** che sfrutta la rete per propagarsi. Si diffonde senza interazioni dell'utente.

BACKDOOR

Permette di accedere **da remoto** ad un pc e a tutte le sue funzioni, ottenendone parziale o completo possesso.

RANSOMWARE

Impedisce l'accesso ad aree del proprio computer, che vengono **bloccate e criptate**. Per ottenere nuovamente l'accesso viene chiesto il pagamento di un **riscatto**.

Malware

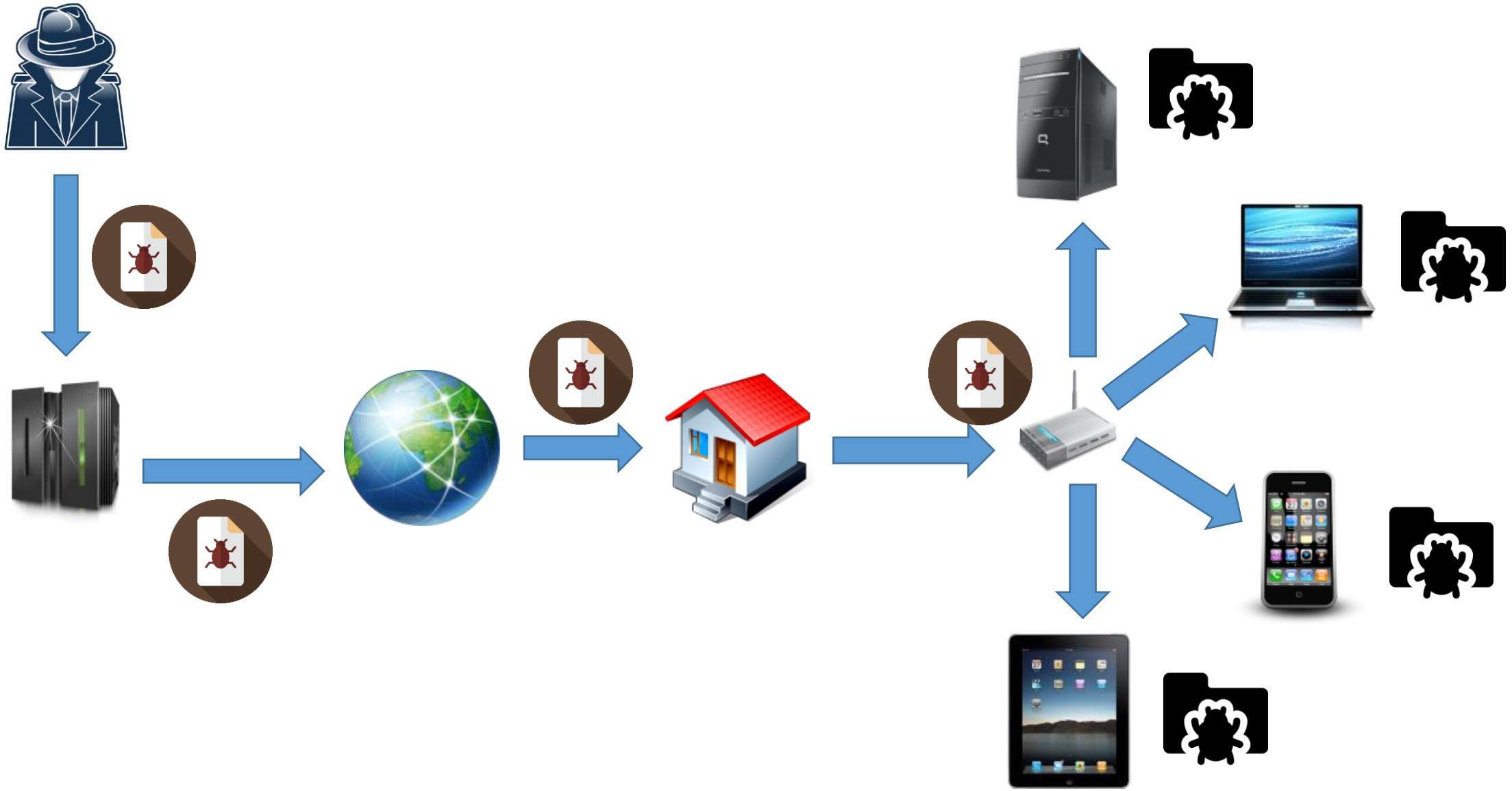
- Con il termine ***malware*** (si intende “programma maligno” o “codice maligno”) si indica genericamente un qualsiasi *software*, creato con lo scopo di causare danni più o meno gravi ad un computer/smarphon/tablet o a un qualsiasi sistema informatico su cui viene eseguito.
- All’interno della categoria dei *malware* si differenziano in varie tipologie: *worm* (“vermi” informatici) o *trojan* (“cavalli di Troia”) nonché a *spyware*, che possono causare la perdita di dati con gravi pregiudizi alla sfera privata.
- Questi programmi agisce con modalità differenti e con obiettivi specifici particolari. Spesso viene fatta confusione tra queste tipologie di virus e malware.

Virus

- Un **virus** è un programma informatico composto da una serie di istruzioni elementari, come qualsiasi altro programma. È solitamente composto da un numero molto ridotto di istruzioni ed è specializzato per eseguire soltanto poche e semplici operazioni ed ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto un file infetto.

Worm

- I **worm** (dall'inglese: "vermi") sono dei programmi opportunamente progettati per danneggiare l'utente, ma, contrariamente ai virus, non necessitano di un programma ospite per funzionare, essendo essi stessi dei programmi completi. Essi sfruttano invece lacune di sicurezza (in gergo "**vulnerabilità**") o errori di configurazione del sistema operativo per propagarsi autonomamente da un computer all'altro.
- Anche in questo caso, il programma, una volta lanciato, può portare a conseguenze estremamente dannose per l'utente: dall'accesso non autorizzato alla macchina da parte di utenti malintenzionati, alla perdita di dati confidenziali, alla totale compromissione del computer.



DIFFERENZE TRA VIRUS E WORM

VIRUS

Frammento di codice **non eseguibile separatamente** da un programma ospite → Deve appoggiarsi ad un altro programma/eseguibile per essere attivato

WORM

Software applicativo a sé che non deve copiarsi in altri file, ma basta che sia eseguito → **Eseguito anche in automatico,** sfruttando vulnerabilità di sicurezza

Trojan

- I **trojan** (letteralmente “cavalli di Troia”) sono programmi che eseguono di nascosto operazioni nocive, nascondendosi all’interno di applicazioni e documenti utili per l'utente. Questi sfruttano lacune di sicurezza dei programmi utilizzati per aprire i file infetti per installarsi nel sistema ad insaputa dell’utente.
- Spesso sono programmi scaricati da internet, altre volte vengono propagati per il tramite di allegati alle Email. I pericoli sono i seguenti: password, codici di accesso ai servizi bancari, pin ecc. Mediante una comunicazione inconsapevole al malintenzionato dei dati digitati sulla tastiera piuttosto che accesso non autorizzato al computer.

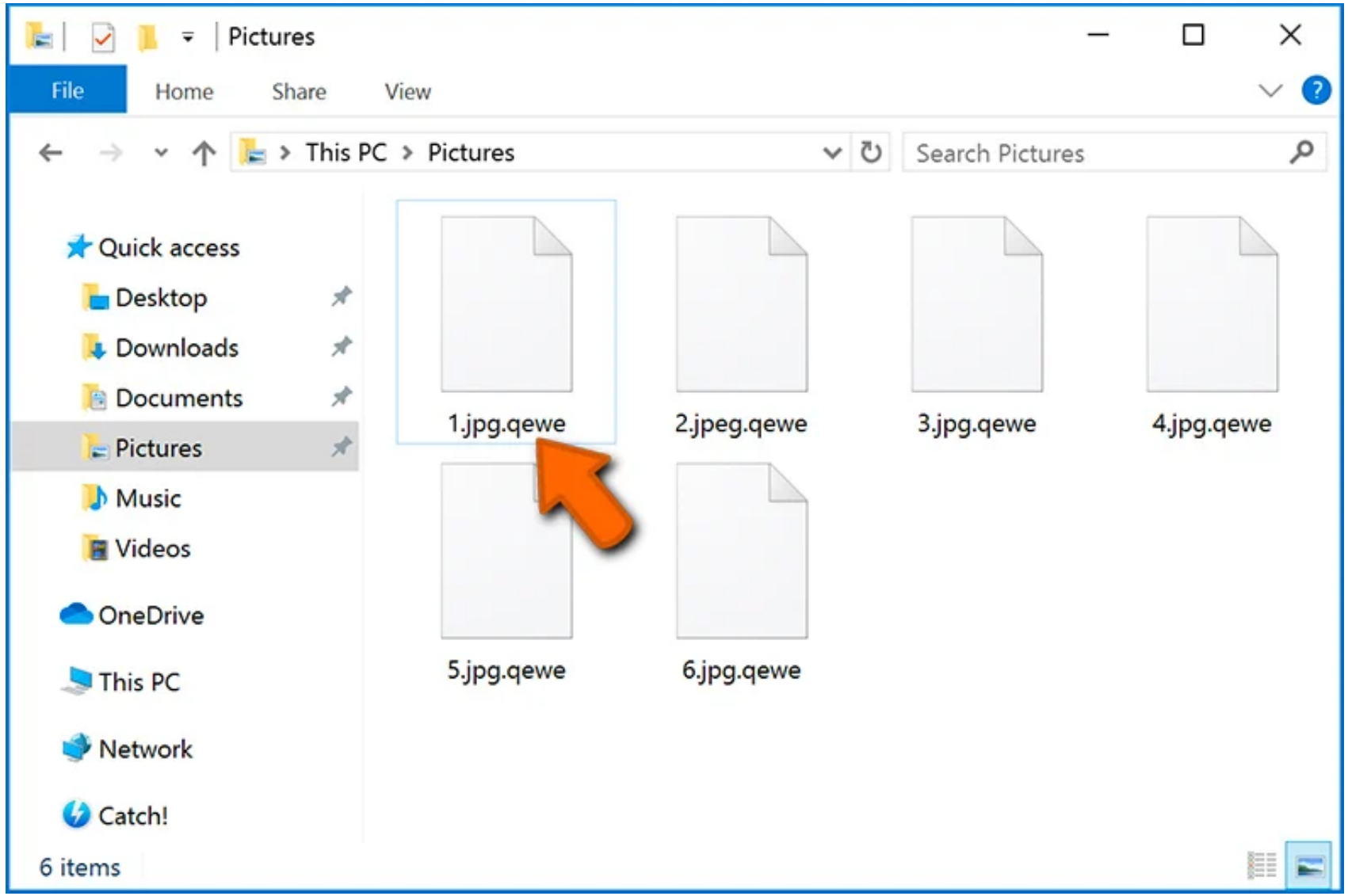
Windows Defender Alert : Zeus Virus Detected In Your Computer !!
Please Do Not Shut Down or Reset Your Computer.
The following data will be compromised if you continue:
1. Passwords
2. Browser History
3. Credit Card Information
4.Local Hard Disk Files.
This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.
Call Technical Support Immediately at (888) 202-7560
Call Microsoft Technical Department: (888) 202-7560 (Toll Free)
SENZAVIRUS

Backdoor

- Una Backdoor permette agli hacker di accedere ad un PC e a tutte le sue funzioni. Vengono settate in modo da superare le difese del sistema ed accedere da remoto al computer, ottenendo con un sistema di crittografia un'autenticazione che permetta di prendere il completo/parziale possesso del terminale. Gli hacker in possesso del computer infetto, utilizzano dei Bot (programmi automatici) che restano dormienti fino a quando non viene eseguito uno specifico comando e che permettono ai criminali informatici di sfruttare il pc per i propri scopi.

Ransomware

- Il ransomware è una forma che impedisce all'utente di accedere a determinate aree del proprio computer. Gli hacker si appropriano dei database (di singoli individui o di intere organizzazioni) e criptano tutti i file in essi contenuti, rendendoli inaccessibili senza chiave di decriptazione. Quando il proprietario tenterà di accedere al database non potrà vederne il contenuto, ma visualizzerà un messaggio che lo forza a pagare per riavere accesso al computer. Per poter ottenere la chiave di decrittazione, gli attaccanti richiedono il pagamento di un riscatto ("ransom").


Pictures
File
Home
Share
View
This PC
Pictures
Search Pictures
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Catch!
1.jpg.qewe
2.jpeg.qewe
3.jpg.qewe
4.jpg.qewe
5.jpg.qewe
6.jpg.qewe
6 items

Altre tecniche per raccogliere informazioni

- Esistono altre tecniche a parte i virus da sfruttate per ottenere informazioni. Alcune sfruttano le nostre ricerche su internet per raccogliere informazioni per poi accedere dati confidenziali.
- Social Engineering
- Vulnerabilità
- Spam
- Chat e instant messaging
- Phishing
- Email
- Cookies
- Wireless lan

PRINCIPALI MEZZI DI INFEZIONE INFORMATICA

DOWNLOAD **SOFTWARE**
E **FILE** CORROTTI
DA **SITI INTERNET**

APP DI **MESSAGGISTICA**
ISTANTANEA
ED **EMAIL**

SUPPORTI PORTATILI
(Chiavette USB, CD,
Hard Disk)

- Scarica software solamente da **siti fidati e certificati**
- Non usare **USB sconosciute**
- **Evita di aprire allegati** mail ricevuti da mittenti sconosciuti/sospetti
- **Non cliccare su link** di cui non conosci la provenienza
- Usa **VPN** soprattutto quando ti connetti da Wi-Fi pubblici

Protezioni

- Sembra che contro questi tipo di virus non ci sia modo di difendersi.
- Invece esistono tecniche ho programmi, per fronteggiare queste minacce quotidiane.
- Istruire utente nel riconosce, virus/hacker

- Antivirus
- Anti-malware
- Software update
- Protezioni dati
- Firewall (No per smarphone/tablet)

Come riconoscere i virus / attacco hacker

- Ora che abbiamo fatto un quadro generico delle tipologie e tecniche per adescare le prede. Cerchiamo di individuare come agiscono i criminali informatici.
- Di solito li piace attaccare le prede tramite finte email di corrieri, siti per le banche oppure sms.
- Il primo passaggio sta nella tipologia di contenuto che ci viene inviata. Esempio: Un criminale ci manda una email riguardo un ordine Amazon. Ma nel testo ci accorgiamo che ci sono lettere accentate dove non dovrebbero esserci e in più si riferisce al plurale ed singolare.
- Cosa facciamo? Per prima cosa non clicco nessun link all'intero della comunicazione. Vado nel sito Amazon per verifica se aspettavamo un ordine.

Da: [redacted] [Mangano_Maury@palestineonline.org] Inviato: venerdì 01/03/2019 11:29
A: [redacted]
Cc:
Oggetto: Relazione di notifica decreto N° 97429021049 del 10.02.2019

Io scrivente Avv. [redacted] con studio a Alba situato in PIAZZA [redacted], 431 P.IVA:40789437961347 nella mia qualità24160749027 di difensore e dom86273929840iciliatario del Sig. [redacted] res. a Venezia indirizzo PIAZZA [redacted]

NOTIFICO16673865759

Ad ogni risultato di legge l'sentenza . 6784673397 in originale informatico

Che lo po scaricare al se37287564306guente indirizzo web - Documenti (ovvero) in copia 08903141488digitale conforme all'originale informatico da me predisposto nel giu84368921007dizio civile dinanzi al Tribunale di Barletta , mediante invio di email di posta elettronica dalla mia casella, e con ricevuta completa, alla tua posta

Attes34485298029to infine che il 91237957378messaggio , oltre al19465205897la presente relata di notifica sottoscritta digital14394141527mente, con54016699396tiene il segue33183926871nte Atto che lo po visualizzare al se54056107719guente link - Atti anch'es57962728764si sottoscritti di55343523126gitalmente: copia informati00993273689ca dell77317146804a atto

Antivirus

- I software “antivirus” proteggono il sistema ed i dati dai virus, dai worm e dai trojan.
- Un software antivirus aggiornato è assolutamente indispensabile se si naviga in internet e si scaricano programmi. Dato che giornalmente nascono numerosi nuovi malware, è tassativamente indispensabile anche un aggiornamento frequente del software antivirus.
- Installare un software antivirus.
- È assolutamente necessario installare una versione aggiornata del software antivirus.
- Aggiornare regolarmente il software antivirus.
- Verificare la validità della licenza.
- Sincerarsi regolarmente che la licenza del software antivirus utilizzato sia ancora valida: il software potrebbe anche continuare a funzionare dopo la scadenza della durata di validità, ma a partire da allora non possono più essere installati gli aggiornamenti.

Marche di Antivirus

Ecco un elenco di antivirus che potete trovare su internet/app, di quelli più conosciuti.

- Avast
- Norton
- Avira
- McAffe
- Avg
- Eset Nod 32
- Kaspersky
- Trendmicro

Sicurezza digitale: video tutorial

- App Avast antivirus per dispositivi android
- App Avast Cleanup per dispositivi android
- Avast antivirus per pc
- Spybot search & Destroy, antispyware per pc
- Social network e piattaforme di videoconferenza

- https://www.comune.modena.it/makeitmodena/news/sicurezza-digitale-video-tutorial

Anti-Malware

- Esistono diversi software di sicurezza informatica, ottimizzati per individuare il malware ed eliminarlo.
  Solitamente, i malware vengono individuati e rimossi con programmi antivirus o anti malware. Si consiglia quindi, di installare un software antivirus di un fornitore affidabile (ad esempio, un'ottima scelta potrebbe ricadere su programmi per malware come gli Antivirus Kaspersky, Malwarebytes o Bitdefender) ed aggiornarlo regolarmente.

kaspersky

Bitdefender

Malwarebytes

Per la casa | Per le imprese | Prezzi | Partner | Risorse | Supporto | Azienda | Effettua il login | DOWNLOAD GRATUITO

Qui troverai tutti i prodotti di sicurezza informatica Malwarebytes scaricabili gratuitamente, compresi gli ultimi strumenti per la rimozione di malware e spyware.

Per la casa

Malwarebytes for Windows

Tecnologia di eliminazione dei malware a più livelli, compresa la protezione contro i virus. Rimozione accurata di malware e spyware. Protezione specializzata contro i ransomware.

SCARICA GRATUITAMENTE

Scopri i prezzi della versione Premium

Malwarebytes for Mac

Protezione proattiva contro malware, ransomware e altre pericolose minacce su quello che sta diventando il computer più amato dagli utenti.

Nota: Solo in inglese

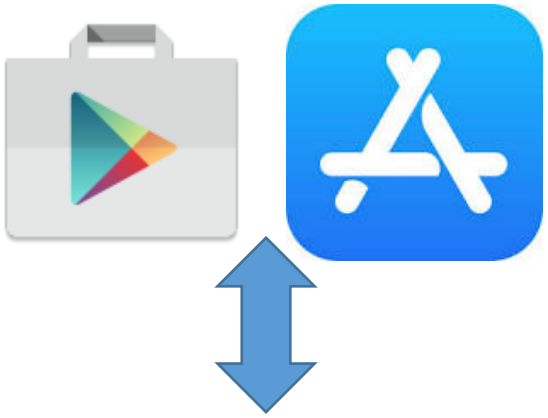
SCARICA GRATUITAMENTE

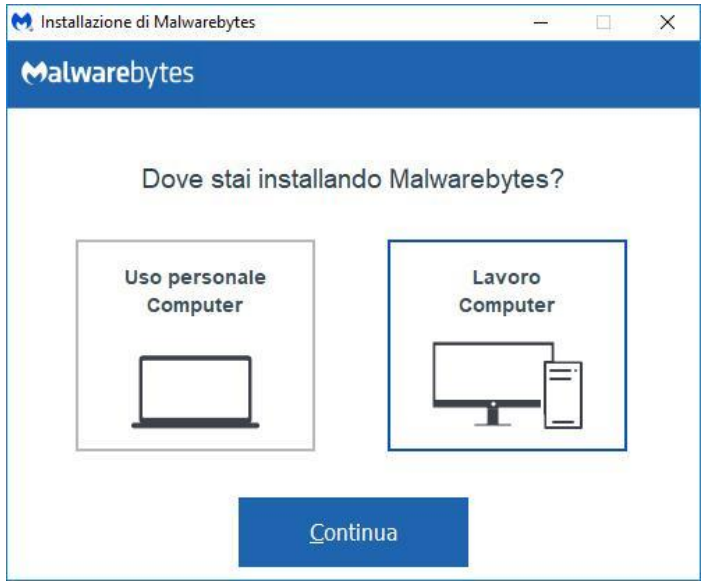
Scopri i prezzi della versione Premium

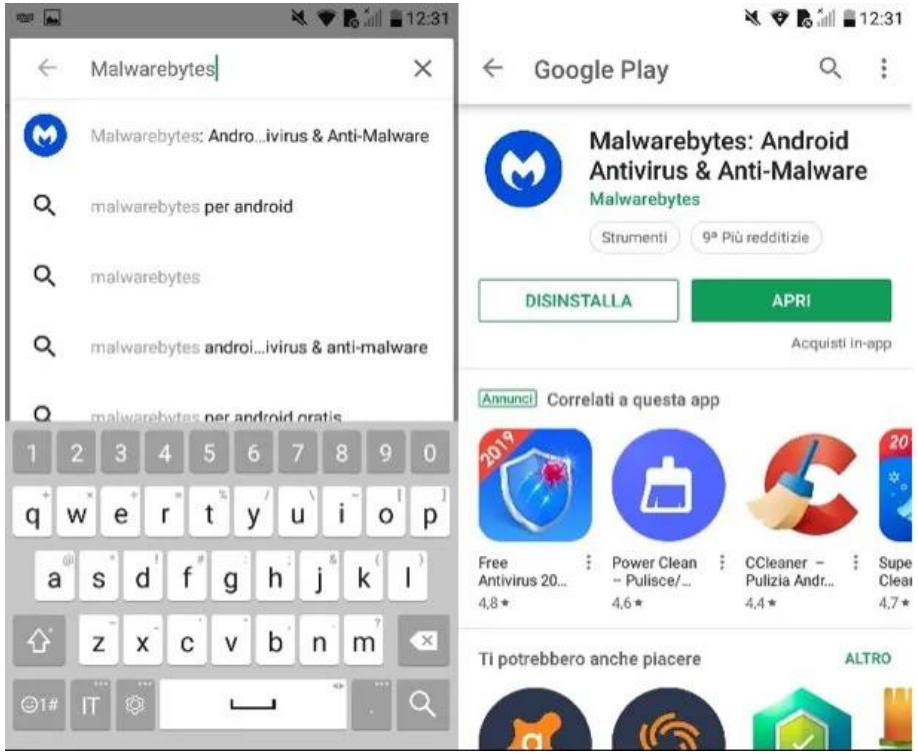
Malwarebytes for Android

Protezione proattiva contro malware, ransomware e altre pericolose minacce su quelli che stanno diventando i dispositivi più diffusi tra gli utenti.

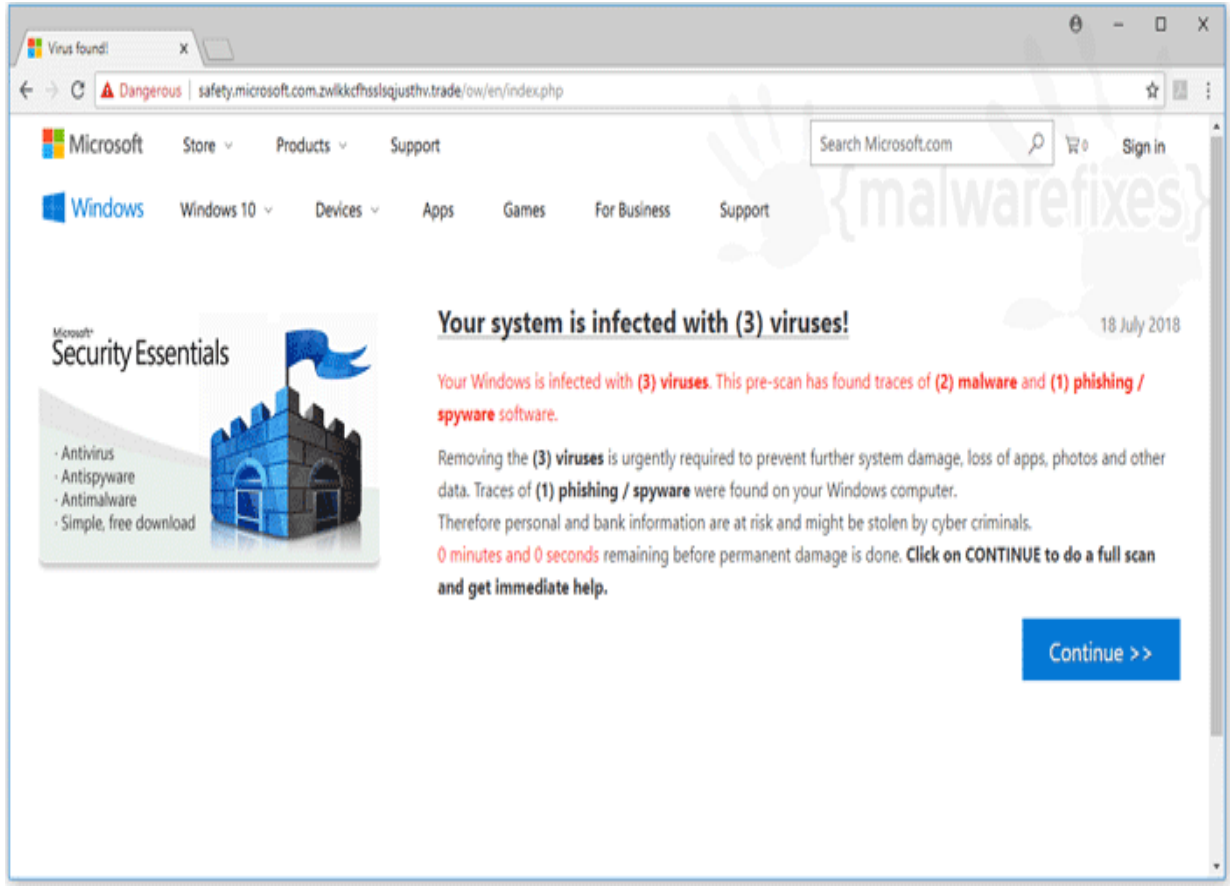
GET IT ON Google play





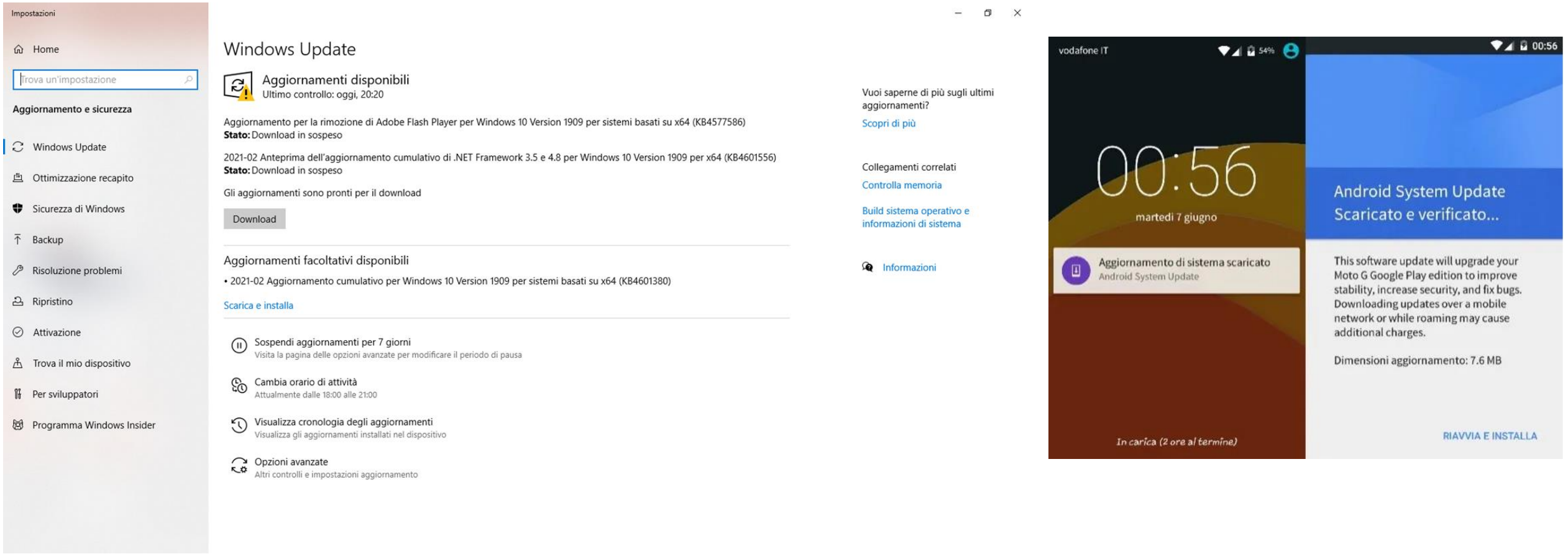


Anche i Browser possono essere infetti



- Anche i browser possono essere infettati dai virus.
- Come rimuoverli? Un buon programma gratuito è Adwclear.
- https://it.malwarebytes.com/adwcleaner/

Software update



Protezione dei dati

- Non può mai essere escluso che i propri dati vengano parzialmente o completamente persi a seguito di errori involontari o inconsapevoli (es. cancellazione del file sbagliato), di problemi tecnici (es. cadute dell'alimentazione elettrica durante il lavoro, anomalie dei programmi) o per colpa di malware presente sul proprio computer. Per ridurre al minimo il rischio di perdita irrimediabile dei dati, è necessario effettuarne regolarmente il salvataggio ("backup") su differenti supporti.
- Backup regolare dei dati
- I dati che si vuole proteggere devono essere copiati periodicamente su supporti esterni (tipicamente CD-ROM, DVD, pennette USB o dischi esterni)
- Conservazione dei dati di backup
- I supporti esterni devono essere conservati in luoghi al riparo e sicuri, teoricamente non nelle dirette adiacenze del computer in uso
- Verifica delle copie di sicurezza
- È sempre buona norma il controllo regolare dell'integrità e della leggibilità dei backup mediante verifica periodica dei file di ripristino contenuti nel backup stesso

Ecco alcuni programmi che si possono usare per fare copie di backup dei vostri computer, sia per dati oppure come copia immagine del hard disk.

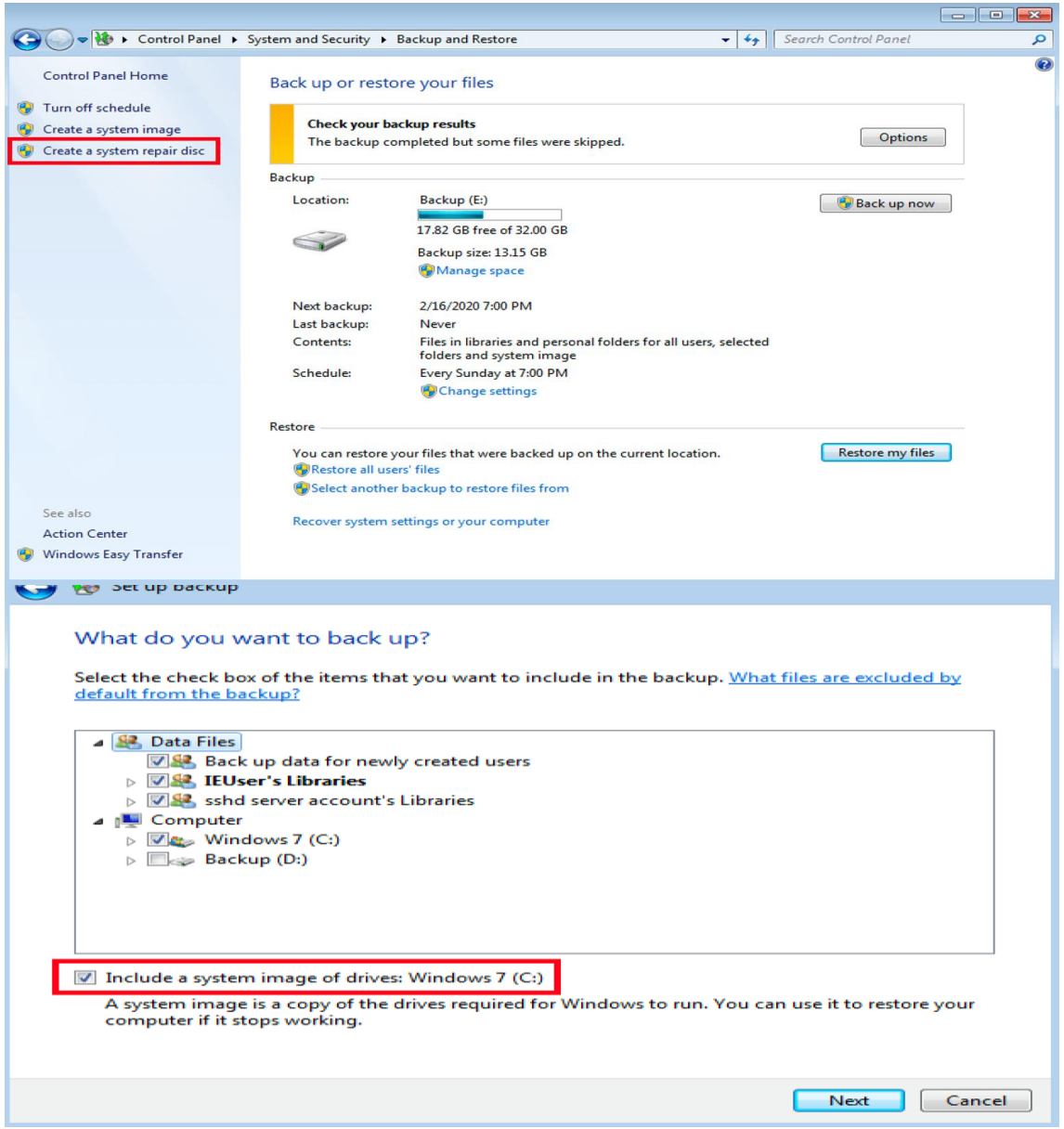
Acronis true image

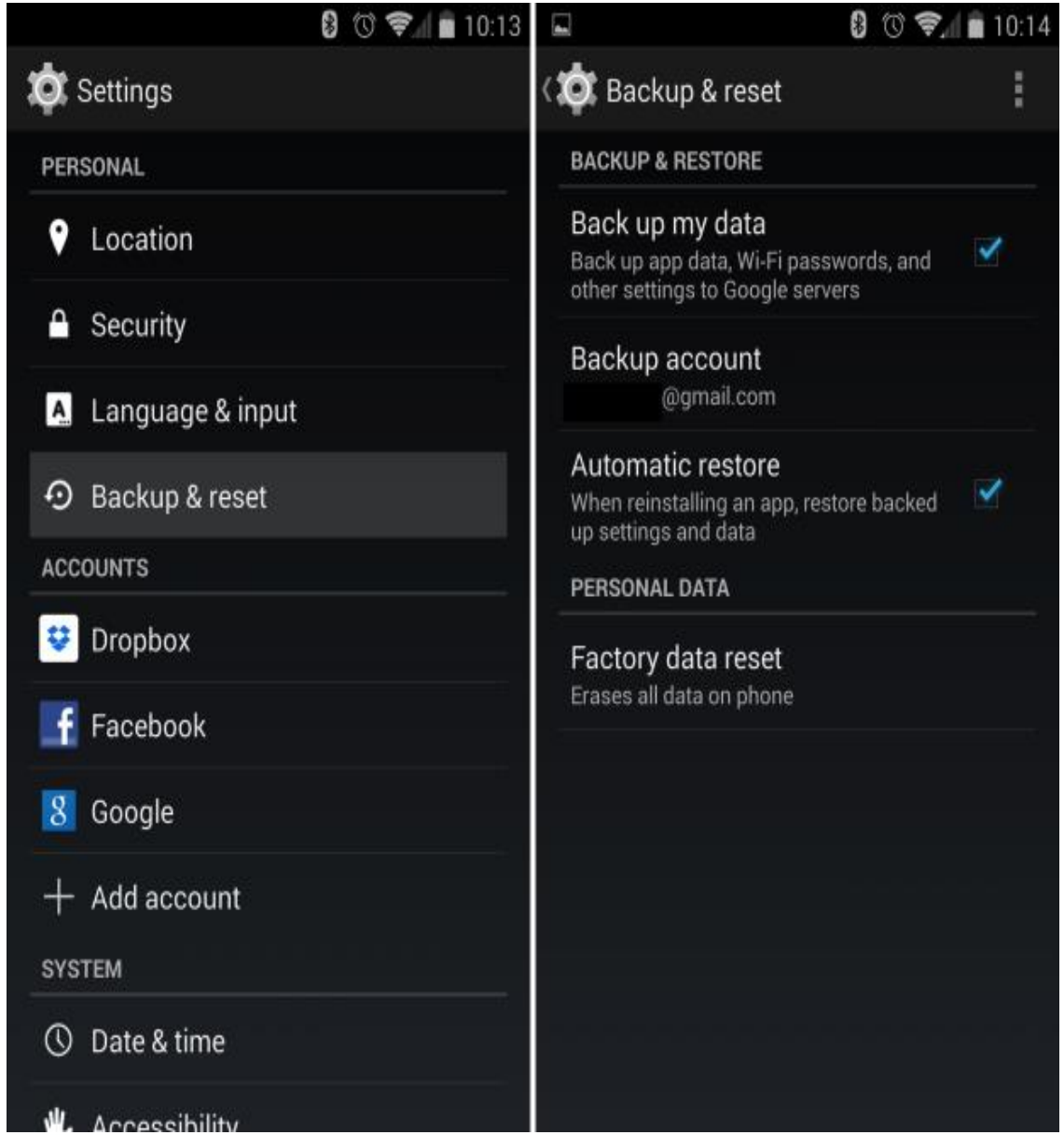
Uranium backup

Aomei partizion backup

Windows backup

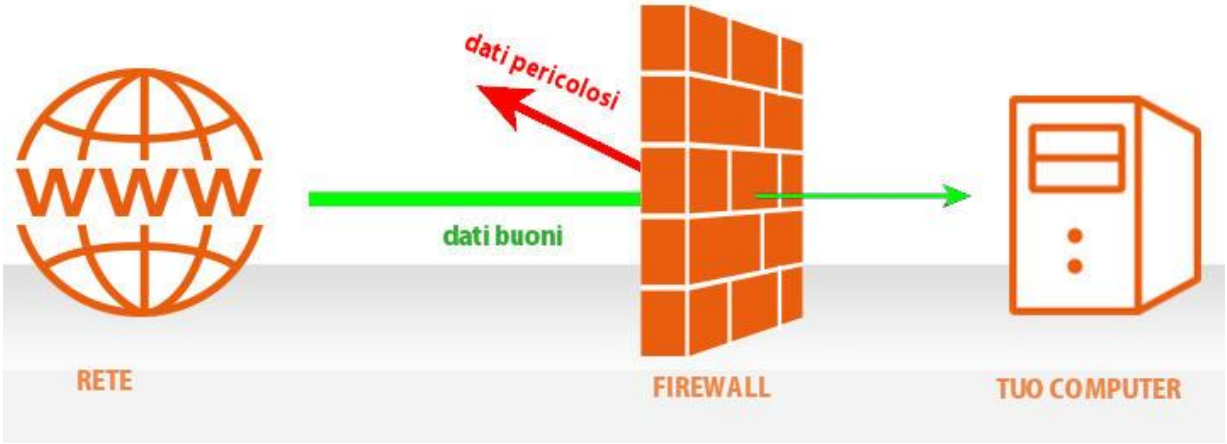
Esistono anche dei servizi online che vi permettono di fare copie di backup, ma principalmente fanno immagini del disco.


Control Panel ▸ System and Security ▸ Backup and Restore
Search Control Panel
Control Panel Home
Turn off schedule
Create a system image
Create a system repair disc
Back up or restore your files
Check your backup results
The backup completed but some files were skipped.
Options
Backup
Location:
Backup (E:)
17.82 GB free of 32.00 GB
Backup size: 13.15 GB
Manage space
Back up now
Next backup: 2/16/2020 7:00 PM
Last backup: Never
Contents: Files in libraries and personal folders for all users, selected folders and system image
Schedule: Every Sunday at 7:00 PM
Change settings
Restore
You can restore your files that were backed up on the current location.
Restore my files
Restore all users' files
Select another backup to restore files from
Recover system settings or your computer
See also
Action Center
Windows Easy Transfer
Set up backup
What do you want to back up?
Select the check box of the items that you want to include in the backup. What files are excluded by default from the backup?
Data Files
Back up data for newly created users
IEUser's Libraries
sshd server account's Libraries
Computer
Windows 7 (C:)
Backup (D:)
Include a system image of drives: Windows 7 (C:)
A system image is a copy of the drives required for Windows to run. You can use it to restore your computer if it stops working.
Next
Cancel


10:13
Settings
PERSONAL
Location
Security
Language & input
Backup & reset
ACCOUNTS
Dropbox
Facebook
Google
Add account
SYSTEM
Date & time
Accessibility
10:14
Backup & reset
BACKUP & RESTORE
Back up my data
Back up app data, Wi-Fi passwords, and other settings to Google servers
Backup account
@gmail.com
Automatic restore
When reinstalling an app, restore backed up settings and data
PERSONAL DATA
Factory data reset
Erases all data on phone

Firewall

- Un **firewall** (“muro tagliafuoco”) controlla i collegamenti entra e uscita dal proprio computer o dalla propria rete ed eventualmente rifiuta le connessioni non autorizzate. Il firewall può essere paragonato a una dogana: la decisione di accettazione o di rifiuto dei collegamenti si basa su regole semplici, verificate ad ogni nuovo collegamento. Grazie al firewall può essere ridotto il rischio di accesso non autorizzato da parte di malintenzionati e minimizzato il pericolo di infiltrazione da parte di worm, trojan o spyware.



Regole di comportamento

- Altri accorgimenti delle tecniche descritte in precedenza (personal firewall, aggiornamenti del software, antivirus), per migliorare la sicurezza del proprio computer è di importanza fondamentale il corretto e consapevole comportamento di ogni singolo utente.
- Tra le regole di base che possiamo suggerire ci sono:
- Buone password
- Prudenza email
- Prudenza navigazione internet
- Configurazione del sistema
- Reti wifi

GLI SPORTELLI NON DA SOLI

S. Faustino, Madonnina
via Leonardo da Vinci, 158 - 41126 Modena
☎ 059 827998 - Fax 059 8303506
Orari di apertura:
dal lunedì al venerdì 9-11
✉ nondasoli.sfaustino@comune.modena.it

Buon Pastore, S. Agnese
via Panni, 202 - 41125 Modena
☎ 059 390431 - Fax 059 390384
Orari di apertura:
dal lunedì al venerdì 9-11.00
✉ anzianibuonpastore@libero.it

Crocetta, San Lazzaro, Modena Est
P.zza Liberazione,13 - 41122 Modena
☎ e fax 059 284109
Orari di apertura:
dal lunedì al venerdì 10-12
✉ nondasoli.modenaest@comune.modena.it

ULTERIORI INFORMAZIONI

Saranno disponibili presso l'Ufficio Politiche per la Legalità e le Sicurezze, il Posto Integrato di Polizia, gli sportelli del servizio **"Non da Soli"**, l'Urp di Piazza Grande e sul sito:
www.comune.modena.it/politichedellesicurezze/non-da-soli

Ufficio Politiche per la Legalità e le Sicurezze
via Scudari, 20 - 41121 Modena
☎ 059 2032502 - 2032431
fax 059 2032109
www.comune.modena.it/politichedellesicurezze/non-da-soli
✉ mosicura@comune.modena.it
PEC modenasicura@cert.comune.modena.it

In collaborazione con:

Prefettura di Modena
Questura di Modena
Guardia di Finanza
Arma dei Carabinieri

Comitato Cittadini Modena Est - Centro Sociale Anziani e Orti Buon Pastore
Centro Sociale Anziani e Orti S. Faustino

Aggiornamento giugno 2017

Comune di Modena
Polizia Municipale

Il Fondo di risarcimento (D.G. n. 317/2017) rientra tra le diverse iniziative del Comune di Modena realizzate per la prevenzione dei reati e per l'aiuto alle vittime, anche in collaborazione con le Forze di Polizia nell'ambito di un protocollo d'intesa finalizzato a migliorare i servizi di aiuto alle vittime

I SERVIZI OFFERTI

☞ FONDO PER IL RISARCIMENTO ALLE VITTIME

Copre i costi sostenuti per:

1) riparazioni di danni materiali arrecati all'abitazione (porta ingresso, portafinestra, finestra) o a sue pertinenze a seguito di effrazioni per furto o tentato furto o sostituzioni a seguito di danni irreparabili.
Risarcimento: 70% della spesa ammissibile fino ad un massimo di € 300,00 anche in presenza di copertura assicurativa privata o condominiale per i danni a carico dell'assicurato in caso di franchigia

2) sostituzione della serratura e rifacimento delle chiavi dell'abitazione della vittima e/o delle sue pertinenze, qualora a seguito di furto, scippo o borseggio sia avvenuto anche il furto delle chiavi.
Risarcimento: 70% della spesa ammissibile fino ad un massimo di € 200,00.

3) sostituzione della serratura o del vetro dei finestrini dell'autoveicolo a seguito di furto o tentato furto su autoveicolo e riproduzione delle chiavi dell'automobile a seguito di furto.
Risarcimento: 70% della spesa ammissibile fino ad un massimo di € 150,00 anche in presenza di copertura assicurativa per la parte dei danni a carico dell'assicurato in caso di franchigia

4) duplicazione di documenti personali rubati (carta d'identità, patente di guida, passaporto, permesso/carta di soggiorno).
Risarcimento: 100% delle spese sostenute per il rifacimento della carta d'identità e la patente di guida;
Risarcimento: 70% delle spese sostenute per il rifacimento del permesso/carta di soggiorno e del passaporto

5) duplicazione di documenti o targhe relativi ad autoveicoli o a ciclomotori a seguito di furto.
Risarcimento: 100% delle spese sostenute

I MODULI DI DOMANDA

Saranno disponibili presso gli Sportelli "**Non da Soli**", presso l'Ufficio Politiche per la Legalità e le Sicurezze o scaricabili dal sito www.comune.modena.it/politichedellesicurezze/non-da-soli

LE DOMANDE DI RISARCIMENTO

Possono essere presentate entro 90 giorni dalla denuncia di reato presso gli Sportelli "**Non da Soli**" o previo appuntamento presso l'Ufficio Politiche per la Legalità e le Sicurezze del Comune; inviate all'indirizzo e-mail mosicura@comune.modena.it; trasmesse al fax dell'Ufficio Politiche per la Legalità e le Sicurezze 059-2032109 e gli sportelli "Non da Soli".

ALTRI SERVIZI DEGLI SPORTELLI

☞ DUPLICAZIONE DI DOCUMENTI

I volontari possono fornirti chiarimenti su come duplicare nella maniera più veloce i documenti più facilmente soggetti a furto.

☞ CONSULENZA LEGALE

I volontari possono aiutarti mettendosi in contatto con alcuni avvocati che possono fornire un parere professionale sulle situazioni che presentano aspetti legali.

☞ SOSTEGNO PSICOLOGICO

I volontari possono darti indicazioni sui servizi utili ad offrirti un sostegno psicologico di tipo professionale.

☞ INFORMAZIONE SUI SERVIZI DEL TERRITORIO

Grazie a contatti con diversi servizi del Comune e di altri Enti, i volontari sono in grado di fornire informazioni su diverse problematiche, e metterti in contatto con i referenti.

FONDO NON DA SOLI

- **Non teniamo denaro o oggetti preziosi** in cassetti o armadi a portata di mano.
- **Durante gli interventi manutentivi** (idraulico, elettricista,...) **facciamo in modo che una persona di fiducia rimanga in casa con noi.**
- **Non buttiamo nella spazzatura le fatture delle utenze (bollette).**
- **Se utilizziamo internet**, diffidiamo di chiunque chieda i nostri dati e credenziali personali (ad es. per sbloccare carte, il bancomat, per verificare se il nostro conto corrente sia stato impropriamente utilizzato, ecc.). **Non comunichiamo mai i nostri dati bancari.**
  Non rispondiamo a e-mail o telefonate contenenti indicazioni Coronavirus.
  Per le notizie e le informazioni sul Coronavirus facciamo solo da le fonti istituzionali facendo riferimento ai siti ufficiali (Ministero della Salute, Istituto Superiore della Sanità, Commissariato di Polizia di Stato, Protezione Civile, Croce Rossa). Evitiamo di diffondere informazioni e notizie tramite messaggi di testo e audio provenienti da fonti diverse.

Se ci sentiamo minacciati o vittime di un reato, telefoniamo al numero unico 112 (Polizia di Stato e Arma dei Carabinieri) o al pronto intervento della Polizia Locale 059 20314

Iniziativa a cura dell'Ufficio Legalità e sicurezze realizzata nell'ambito del progetto "La prevenzione rende sicuri: azioni integrate per il contrasto di truffe e raggiri ai danni della popolazione anziana" finanziato dal Fondo Unico di Giustizia del Ministero degli Interni, con la collaborazione di:

- Sportelli di aiuto alle Vittime di Reato "Non da Soli"
- Sportello S.O.S. Truffa & C.
- Associazioni dei Consumatori

Comune di Modena
Ufficio Legalità e Sicurezze
Via Scudari, 20 - Modena
tel. 059 2032502-2032963
fax 059 2032109
mosicura@comune.modena.it
www.comune.modena.it/politichedellesicurezze

In banca, in posta, nei negozi, al mercato

- **Facciamo accreditare la pensione** sul conto corrente o sul libretto di risparmio e paghiamo le utenze tramite accredito sul conto corrente (domiciliazione utenze).
- **Non rechiamoci in banca o in posta** in orari di punta; se possibile, chiediamo ad un parente o conoscente di di accompagnarci.
- **Quando utilizziamo il bancomat:** accertiamoci che nessuno possa vedere il codice pin. Preleviamo l'importo minimo necessario e riponiamo immediatamente la somma.
- **Non teniamo il codice pin in evidenza.**
- **Non distraiamoci** mentre paghiamo o maneggiamo il denaro.
- **Non parliamo di operazioni di deposito o prelievo,** soprattutto se nelle vicinanze ci sono sconosciuti che ci ascoltano.
- **Non facciamoci avvicinare da estranei** quando usciamo dalla banca o dalla posta, anche se si presentano come colma dipendenti e con una scusa ci vedono di controllare il nostro denaro.
- **Quando facciamo la spesa** non lasciamo mai borse o borsetti incustoditi sul carrello. Dopo aver fatto la spesa, mentre carichiamo le buste sull'auto, non lasciamo la borsa incustodita sui sedili. **Chiudiamo a chiave l'auto** quando andiamo a riporre il carrello.

In autobus, bicicletta o in automobile

- **Sull'autobus,** non ci lasciamo avvicinare da sconosciuti. Qualche malintenzionato potrebbe sfilarci il portafoglio dalle tasche posteriori o dalla borsa. Teniamo la borsa a tracolla e lo zaino davanti.
- **In bicicletta,** non mettiamo mai la borsa sul manubrio, nel cestino o nel portapacchi, ma indossiamola a tracolla.
- **Chiudiamo sempre a chiave l'auto,** anche se ci allontaniamo per pochi istanti, e non lasciamo mai all'interno oggetti che possono attirare l'attenzione come borse, giacche, oggetti di valore.
- **Facciamo attenzione a chi si rende disponibile** a darci una mano per aiutarci (gomma bucata) o ci contesta un danno subito (specchietto rotto, danno alla carrozzeria), nel dubbio chiamiamo le Forze di Polizia.
- Portiamo con noi **solo il denaro indispensabile.**

Quando camminiamo per strada

- Sul marciapiede, **teniamo la borsa o il borsello a tracolla e dal lato interno,** camminando vicino al muro per scoraggiare eventuali malintenzionati.
- **Evitiamo la folla** perché i borseggiatori possono approfittare del contatto fisico per derubarci.
- **Non ascoltiamo** chi ci avvicina chiedendoci di pagare un debito contratto da un parente (figlio, nipote) e non consegniamo per nessun motivo denaro: chiamiamo immediatamente il numero di emergenza 112 e chiediamo aiuto ai passanti.
- **Se abbiamo il sospetto** di essere seguiti entriamo nel negozio più vicino.
- **Non accettiamo** di vedere cataloghi di articoli vari.
- **Non firmiamo** mai nulla.
- **Non comunichiamo** i nostri dati personali.

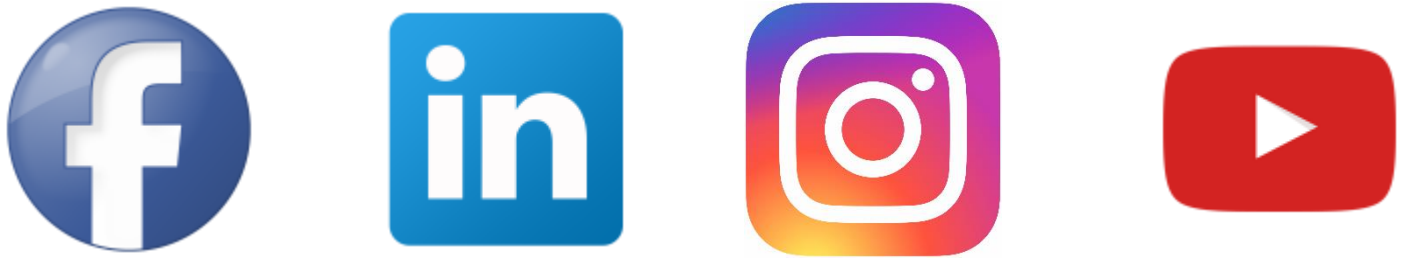
Quando siamo a casa

- **Se una persona sconosciuta** vuole salire in ascensore con noi, diciamo che aspettiamo una persona o ci accertiamo della motivazione della sua presenza.
- **Non lasciamo i bambini** liberi di aprire la porta.
- **Quando rientriamo** a casa stiamo attenti che nessuno ci segua, chiudiamo la porta e non lasciamo la chiave nella serratura. Inseriamo il chiavistello se la nostra porta ne è fornita.
- **Non apriamo agli sconosciuti.** Gli operatori di acqua, luce, gas, telefonia e degli Enti pubblici sono riconoscibili da un tesserino ben visibile e preannunciano il loro arrivo. Non siamo obbligati ad aprire, i consumi possono essere comunicati successivamente con l'aiuto di un parente o amico.
  Non apriamo a chi vuole venderci vaccini o farmaci specifici per prevenire o curare il coronavirus in quanto non sono ancora in commercio e non verranno distribuiti a casa senza preavviso.
- **Se non siamo sicuri della loro identità,** non apriamo neppure a chi si presenta in divisa delle Forze di Polizia. **Nel dubbio contattiamo il numero di emergenza 112.**
  Allo stesso modo non apriamo a chi si presenta come infermiere, incaricato di ASL o di Pubblica Amministrazione per somministrare il tampone per il Coronavirus se non siamo stati prima preavvisati.
- **Non facciamo entrare in casa persone** che dicono di essere state mandate dall'amministratore di condominio, dal vicino, da un parente, dalla banca o che dicono di dovere entrare per risolvere problemi vari (perdite d'acqua, controllo banconote ecc.).
- **Non apriamo a chi si presenta per eseguire** disinfestazioni da coronavirus delle abitazioni e dei condomini.

→

Associazione MODI:

- https://www.associazionemodi.it/



- @modiaps