TUTELARSI DA INTRUSIONI E ABUSI

Luca Cadonici
Membro ONIF – Osservatorio Nazionale sull'Informatica Forense
Docente European Forensic Institute (Malta)
Docente Istituto Italiano di Scienze Forensi

La violenza online: come riconoscerla
e come difendersi
22 ottobre 2022

1 Introduzione alla Sicurezza Informatica

- **Insieme di mezzi, tecnologie, attività e processi** tesi alla **protezione** dei beni e degli *asset* informatici, ovvero dei **dati** da essi contenuti, elaborati e scambiati.

- La sicurezza informatica è, prima di tutto, sicurezza del **dato**.

- Ad oggi non si può più prescindere dall'estendere e integrare la **sicurezza fisica** con la sicurezza delle **informazioni**.

2) LE PRINCIPALI TIPOLOGIE DI MINACCIA INFORMATICA

2 Minacce informatiche

- Fanno leva sui punti deboli dei **dispositivi**, delle **applicazioni** e, soprattutto degli **utenti**
- L'essere umano è l'anello **debole** della catena
- L'essere umano è l'elemento **meno controllabile**
- Necessità di **consapevolezza**, di **regole** e di **formazione**

2.1 Minacce informatiche

Malware

- *Malicious Software* (Codice Maligno)
- Programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata
- Programma in grado di apportare danni a un sistema informatico o impedirne l'uso
- Programma in grado sottrarre informazioni riservate

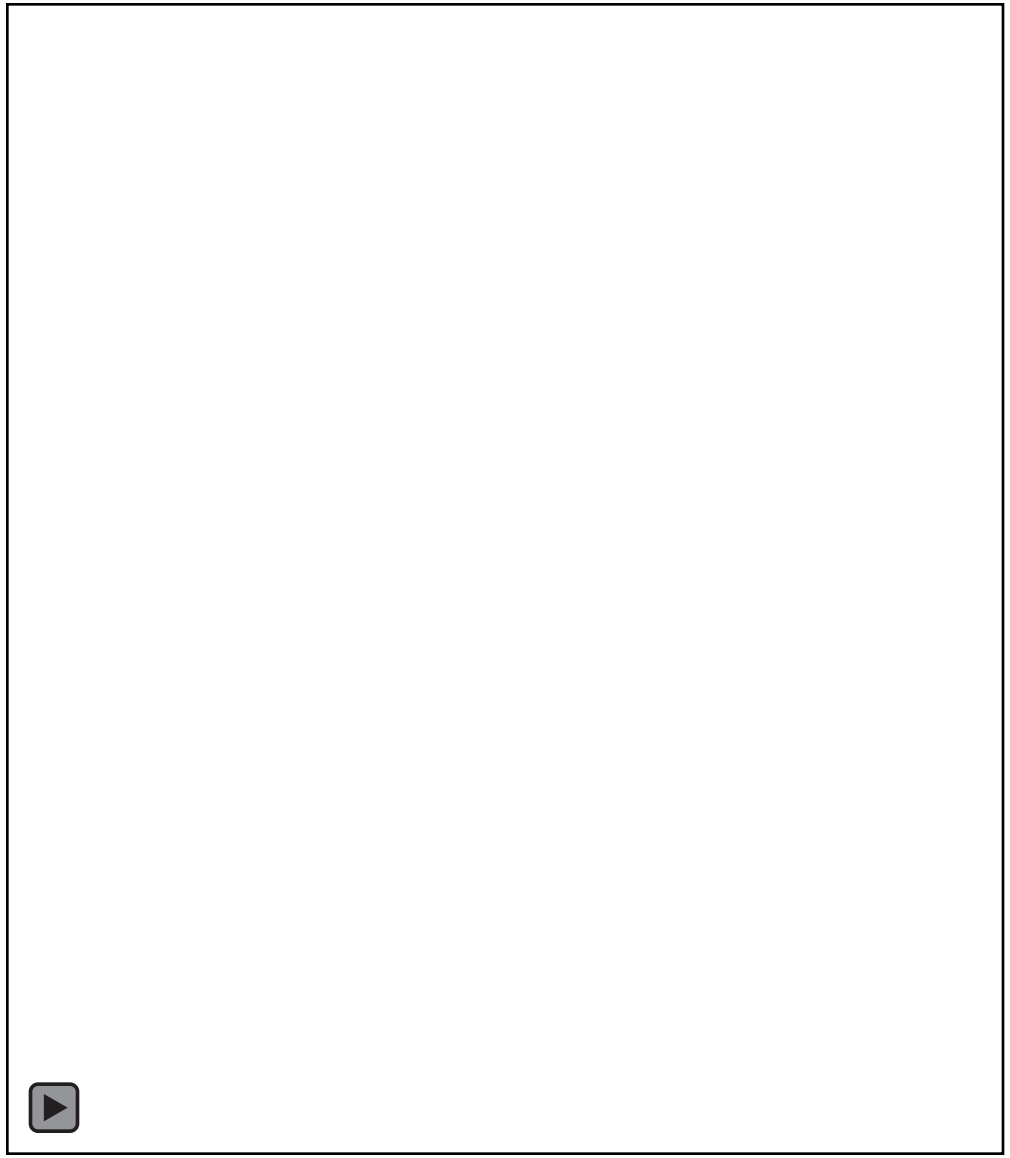
2.2 Minacce informatiche

Phishing

- Metodo di frode in cui viene presentato un **messaggio apparentemente proveniente** da un **ente affidabile** in una comunicazione digitale, per indurre la vittima a divulgare informazioni riservate, quali **dati finanziari** o **codici di accesso**.

2.3 Minacce informatiche

Phishing



2.3 Minacce informatiche

Spear Phishing

- Phishing realizzato mediante l'invio di messaggi mirati
- Vengono inviati a un numero ristretto di persone
- Sembrano provenire da amici, clienti, fornitori, collaboratori professionali
- Contengono informazioni vere sulla vittima e su i suoi comportamenti

2.3 Minacce informatiche

Spear Phishing

- Attività pregressa di analisi dei comportamenti e delle conoscenze della vittima (*OSINT*, *Social Engineering*)
- Prima di sferrare l'attacco, il nostro comportamento viene analizzato sui social
- Basandosi su queste ricerche, i malintenzionati creano messaggi estremamente mirati pertinenti alla vita della vittima

3) PROTEZIONE CREDENZIALI DI AUTENTICAZIONE

3. Protezione credenziali

- L'**identità digitale** è l'insieme delle risorse digitali associate in maniera univoca ad una persona fisica che la identifica, rappresentandone la volontà, durante le sue attività digitali.
- L'identità digitale, di norma, viene presentata per accedere ad un sistema informatico o ad un sistema informativo o per la sottoscrizione di documenti digitali.
- In un'accezione più ampia essa è costituita dall'insieme di informazioni presenti online e relative ad un soggetto.

3. Protezione credenziali

- L’accesso all’identità digitale e ai servizi ad essa connessi (mail, social etc.) passa dal possesso di determinate **credenziali di autenticazione**.
- Nella forma più semplice le credenziali di autenticazione sono username e password, ovvero un **codice univoco di identificazione** (*username*) ed un codice in esclusivo possesso del titolare dell’identità digitale (**password**), sostituibile o associabile ad una caratteristica biometrica (*Touch ID*, *Face ID*) o ad un dispositivo (*token fisico* o *digitale, generatore OTP, smart card*).

3.1 Gestione e complessità delle password

- **Sicurezza delle password**:
  - Lunghezza
  - Maiuscole e minuscole
  - Numeri
  - Caratteri speciali
- Non utilizzare parole o frasi di senso compiuto
- Non utilizzare riferimenti a persone o date
- Mai conservare le password in chiaro (su file di testo non cifrati o su fogli di carta)
- Utilizzare software o hardware per la conservazione e gestione delle password
- Stabilire una routine di cambio delle password
- Stabilire requisiti minimi di complessità delle password

3.1 Gestione e complessità delle password

- Sicurezza delle password:
  - Lunghezza
  - Maiuscole e minuscole
  - Numeri
  - Caratteri speciali

Resistenza ad attacchi a «forza bruta»

- Non utilizzare parole o frasi di senso compiuto
- Non utilizzare riferimenti a persone o date
- Non usare password «comuni» (es. *password*, *qwerty*, *123456* etc.)

Resistenza ad attacchi a «dizionario»

- Mai conservare le password in chiaro
- Utilizzare software o hardware per la conservazione e gestione delle password

Resistenza a furto di credenziali

3.1.1 Gestione e complessità delle password

Attacchi a forza bruta

- **Attacco a forza bruta**
- Metodo utilizzato da un attaccante per individuare una password di accesso ad un sistema provando in maniera esaustiva tutte le possibili combinazioni di caratteri ammesse e tutte le lunghezze di stringa ammesse dal particolare sistema.
- Il successo dipende da 4 fattori:
  - **Lunghezza** della password
  - **Complessità** della password
  - **Tempo** a disposizione
  - **Risorse computazionali** dell'attaccante

3.1.2 Gestione e complessità delle password

Attacchi a dizionario

- **Attacco a dizionario**
- Differisce dall'attacco a forza bruta perché, anziché provare tutte le combinazioni di lettere, numeri e caratteri speciali, fa riferimento a un numero finito di parole in un dizionario specifico

- Non utilizzare parole o frasi di senso compiuto
- Non utilizzare riferimenti a persone o date

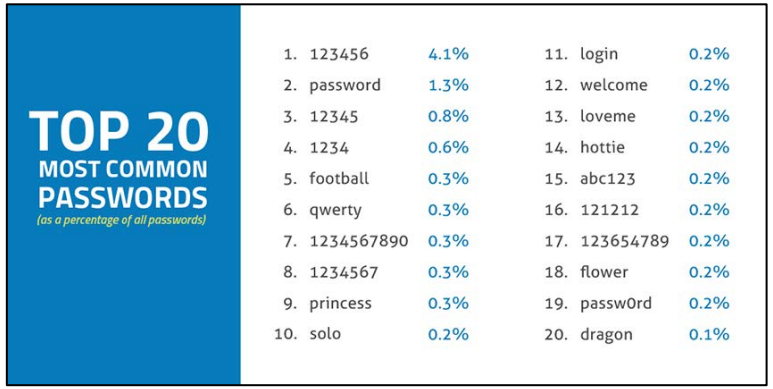
Resistenza ad attacchi a «dizionario»

- I dizionari possono essere creati *ad hoc* utilizzando i dati personali dell'utente (date importanti, nomi di familiari etc.)
- In rete sono reperibili dizionari di password comuni o di default utilizzabili per questo tipo di attacco

3.1.2 Gestione e complessità delle password

Attacchi a dizionario

- **Attacco a dizionario**



3.1.3 Gestione e complessità delle password

Furto di credenziali

- **Furto di credenziali**
  - Non **visualizzare** le password in chiaro
    - **Shoulder surfing:** tecnica di **social engineering** che consiste nell'osservare l'utente mentre digita le proprie credenziali
  - Non **conservare** le password in chiaro
    - **Password sniffing:** esistono software in grado di recuperare le password salvate in chiaro nei browser
  - Non **salvare** le password su file di testo
    - Facilmente recuperabili con una semplice indicizzazione di contenuti
  - Non conservare le password su quaderno o foglio di testo in giro per casa o ufficio
  - Conservare in cassaforte le password stampate da usare in caso di emergenza
  - Distruggere qualunque supporto cartaceo dove sono state memorizzate password
    - **Dumpster diving:** tecnica di **social engineering** che consiste nel frugare nei cestini cercando password annotate su supporti cartacei

3.2 Password manager

- **Password manager**
  - Strumenti software o hardware che archiviano username e password del proprietario in **maniera cifrata**
  - Sono protetti da una **Master Password** necessaria per accedere alle password memorizzate
  - Pertanto è sufficiente che l'utente memorizzi un'unica password per accedere alle credenziali memorizzate
  - La **master password** può essere eventualmente sostituita da PIN, token di autenticazione o dati biometrici nei *password manager* più evoluti

3.2 Password manager

- **Password manager**
  - Tre tipologie di password manager:
    - Web

      Credenziali memorizzate su **server di terze parti** (*1Password, LastPass, iCloud Keychain*)
    - Software

      Credenziali memorizzate sui **dispositivi dell'utente** (*KeePass*, *browser web*)
    - Hardware

      Credenziali memorizzate sui **dispositivi di accesso** (*YubiKey*, *OnlyKey*)

3.2.1 Password manager software

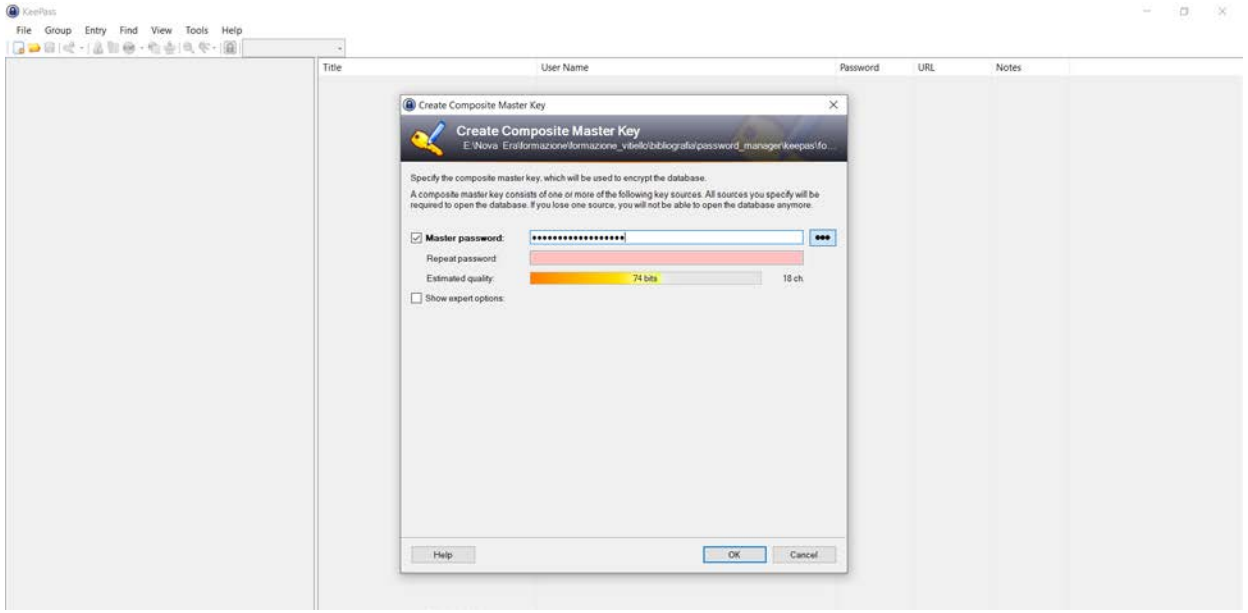
KeePass 2

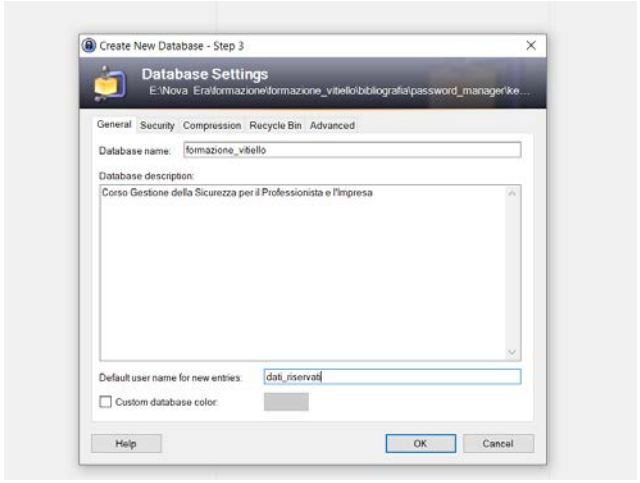
- **KeePass 2**
- Estrema facilità d'uso
- Genera file .kdbx che possono essere copiati o trasferiti in sicurezza
- Username e password vengono copiati direttamente nella *clipboard*
- Genera automaticamente password complesse
- Permette di impostare una data di scadenza delle password
- Mostra una valutazione sulla sicurezza di ogni password
- Protezione aggiuntiva grazie alla funzione **Lock Workspace**
- Disponibile anche per mobile tramite l'app *KeePass Touch*

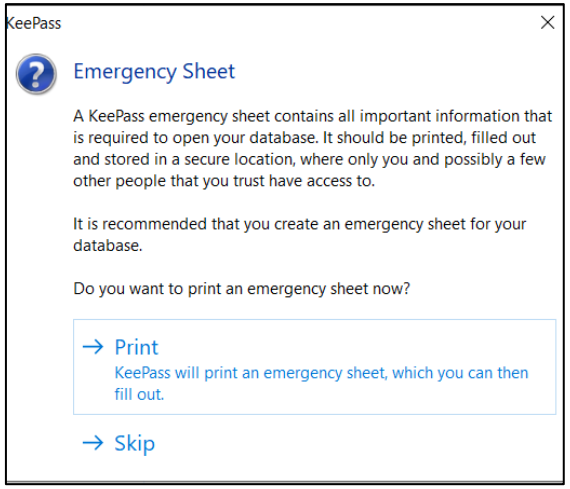
3.2.1 Password manager software

KeePass 2

- **KeePass 2**



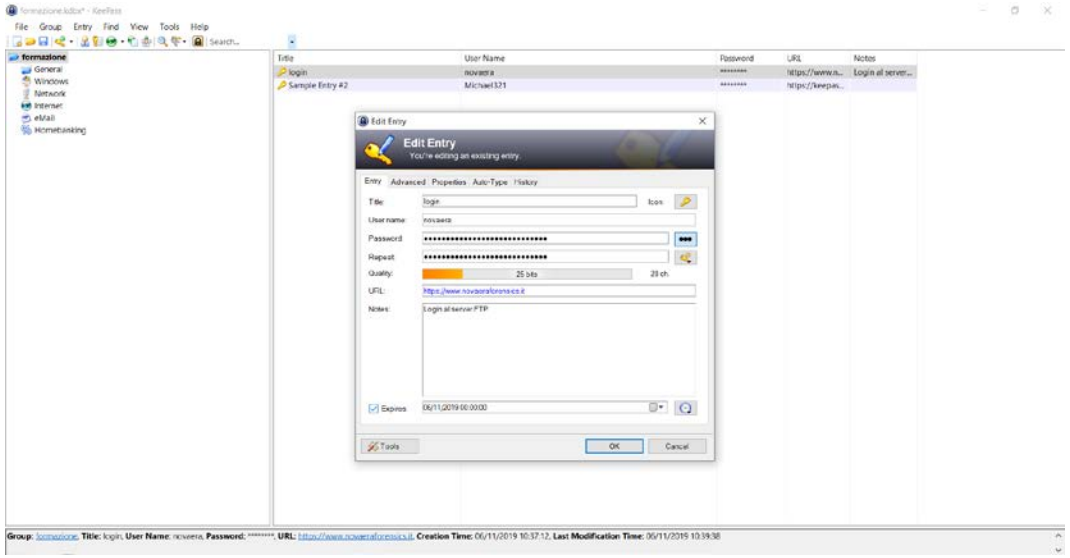


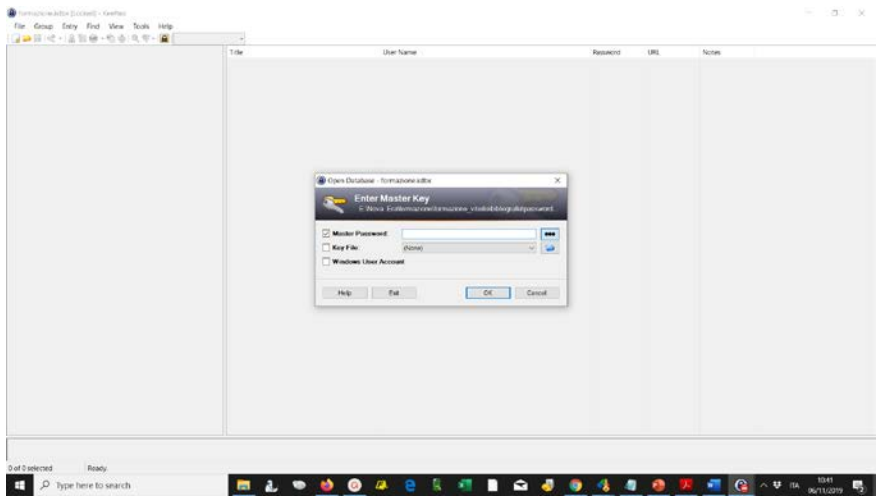


3.2.1 Password manager software

KeePass 2

- **KeePass 2**

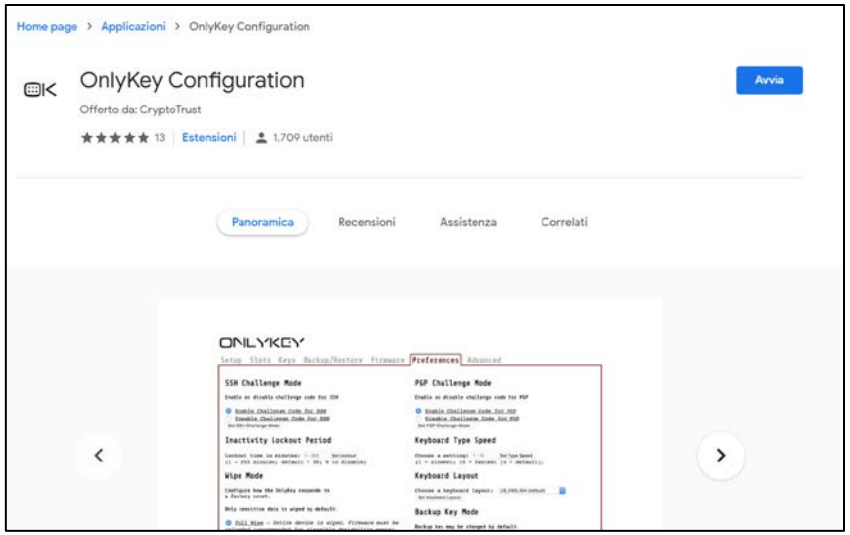




3.2.2 Password manager hardware

OnlyKey

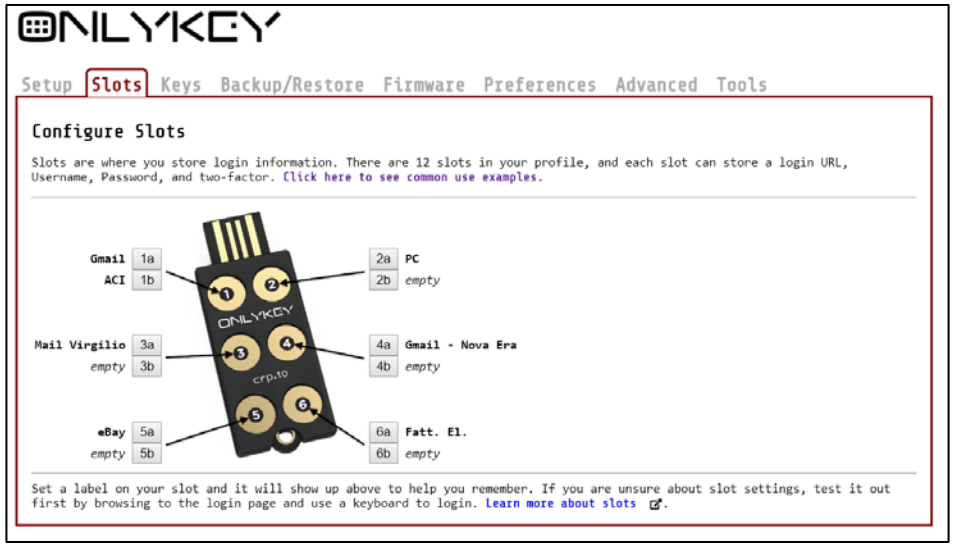
- **OnlyKey**
- Storage offline delle password
- Protetto da PIN
- Supporta autenticazione a due fattori
- Configurabile tramite estensione per *Chrome* o direttamente alla prima connessione
- OpenPGP

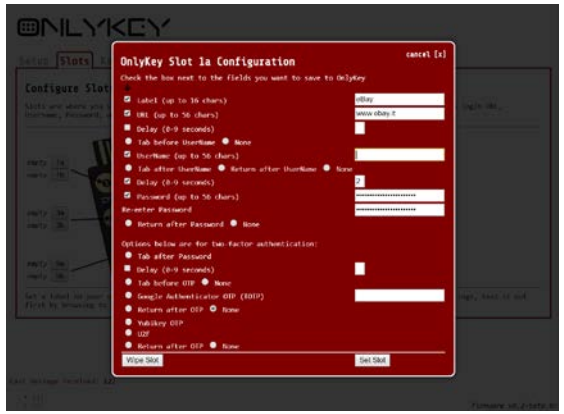


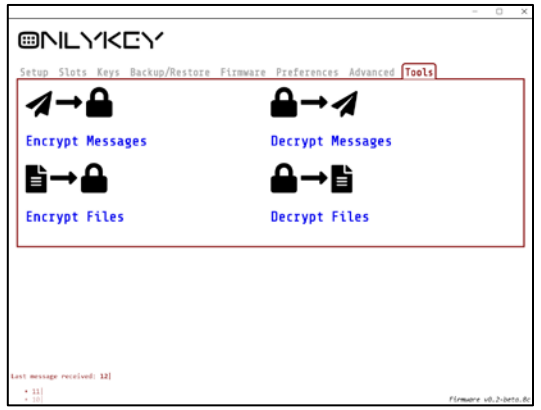
3.2.2 Password manager hardware

OnlyKey

- **OnlyKey**
- 6 tasti
- 12 slots
- Ogni slot può memorizzare URL, username, password



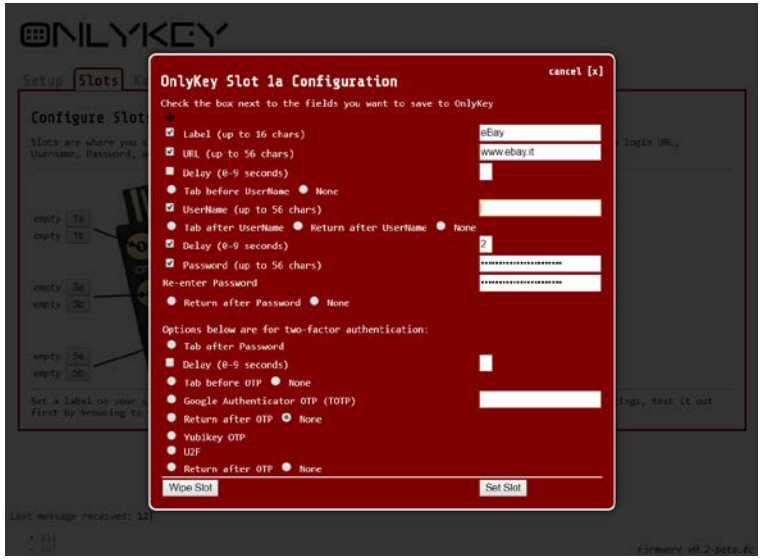


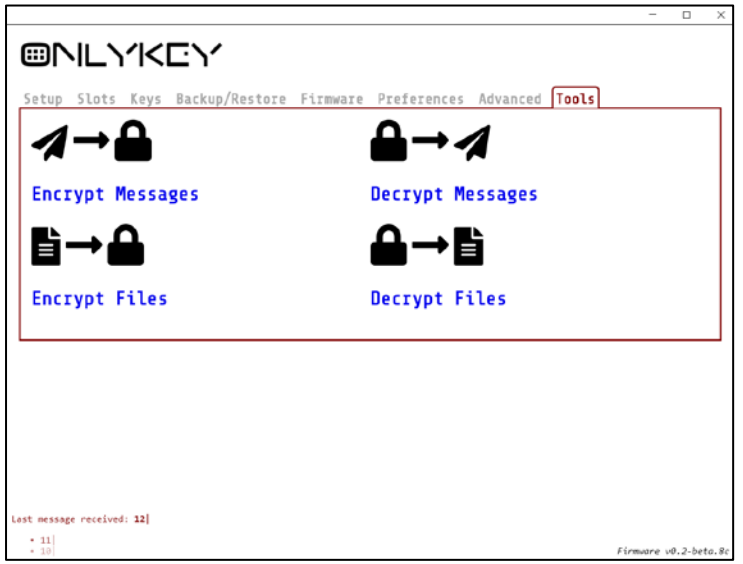


3.2.2 Password manager hardware

OnlyKey

- **OnlyKey**
- 6 tasti
- 12 slots
- Ogni slot può memorizzare URL, username, password, e dati dell'autenticazione a 2 fattori

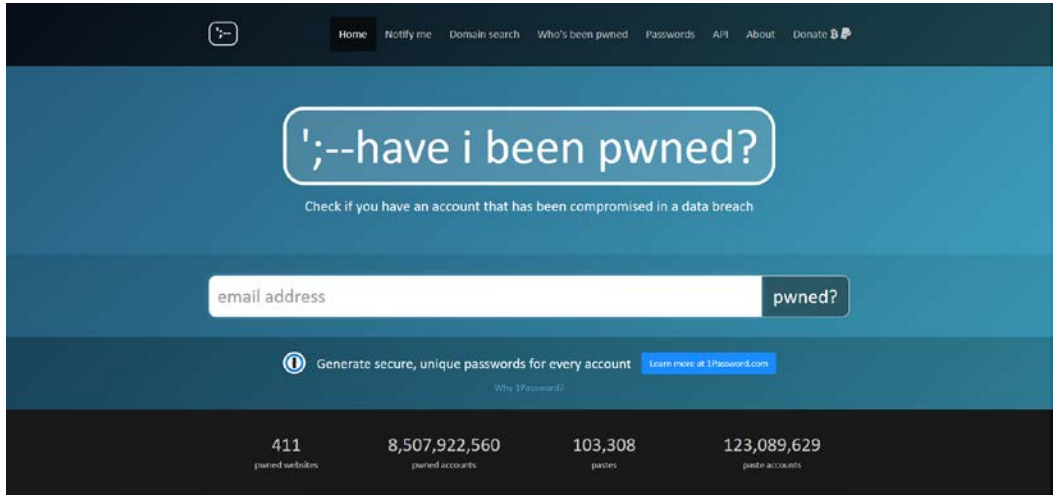




3.3 Verifica compromissione email

haveibeenpwned.com

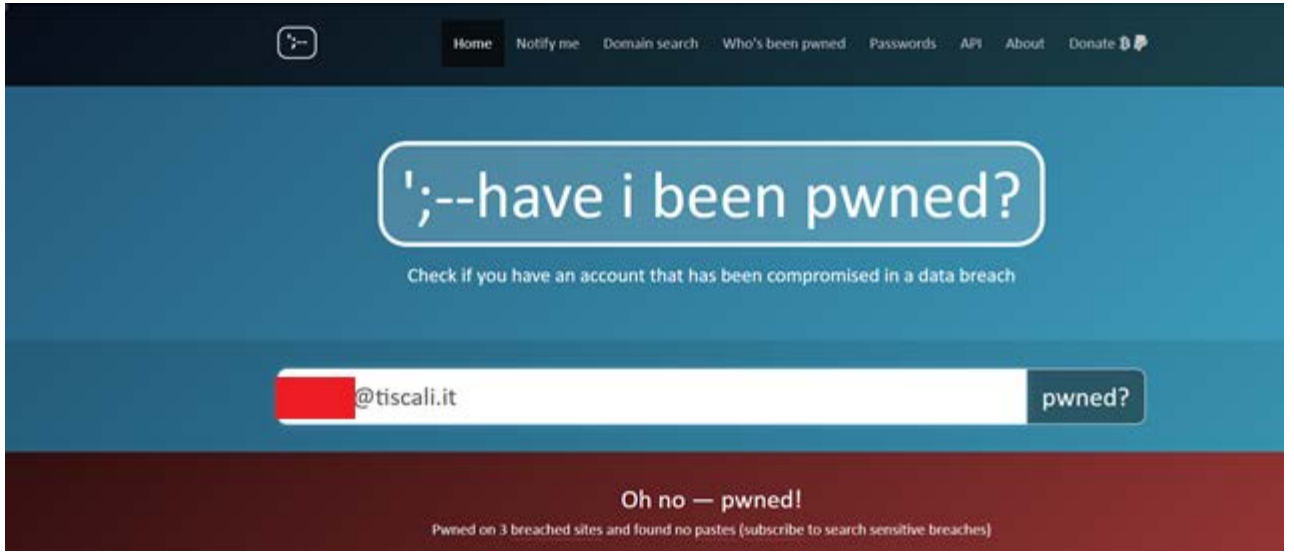
- **haveibeenpwned.com**
- Sito Web che consente agli utenti di Internet di verificare se i loro dati personali sono stati compromessi da violazioni dei dati.
- Il servizio raccoglie e analizza dozzine di *dump* e *paste* di database contenenti informazioni su centinaia di milioni di account trapelati
- Consente agli utenti di cercare le proprie informazioni inserendo il proprio nome utente o indirizzo e-mail.
- **<u>Fondamentale per verificare la compromissione dei propri indirizzi mail e degli account ad essi associati</u>**

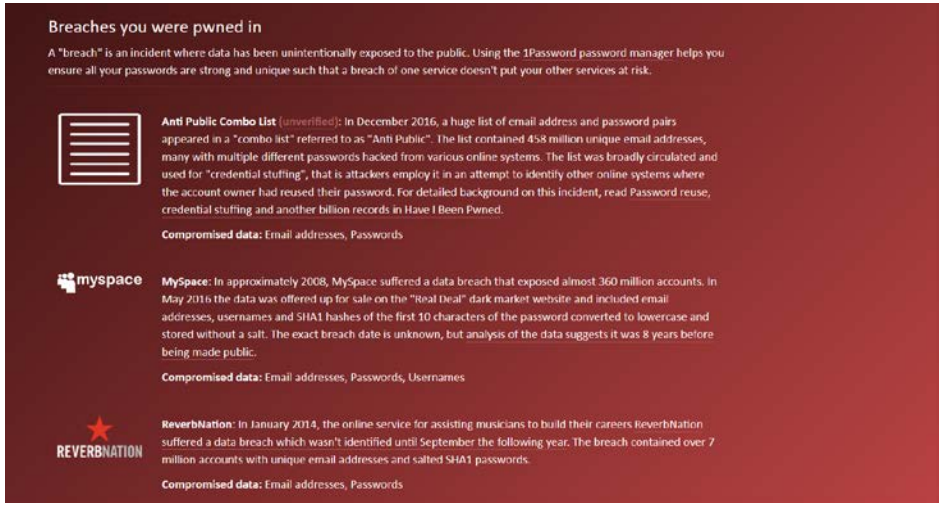


3.3 Verifica compromissione email

haveibeenpwned.com

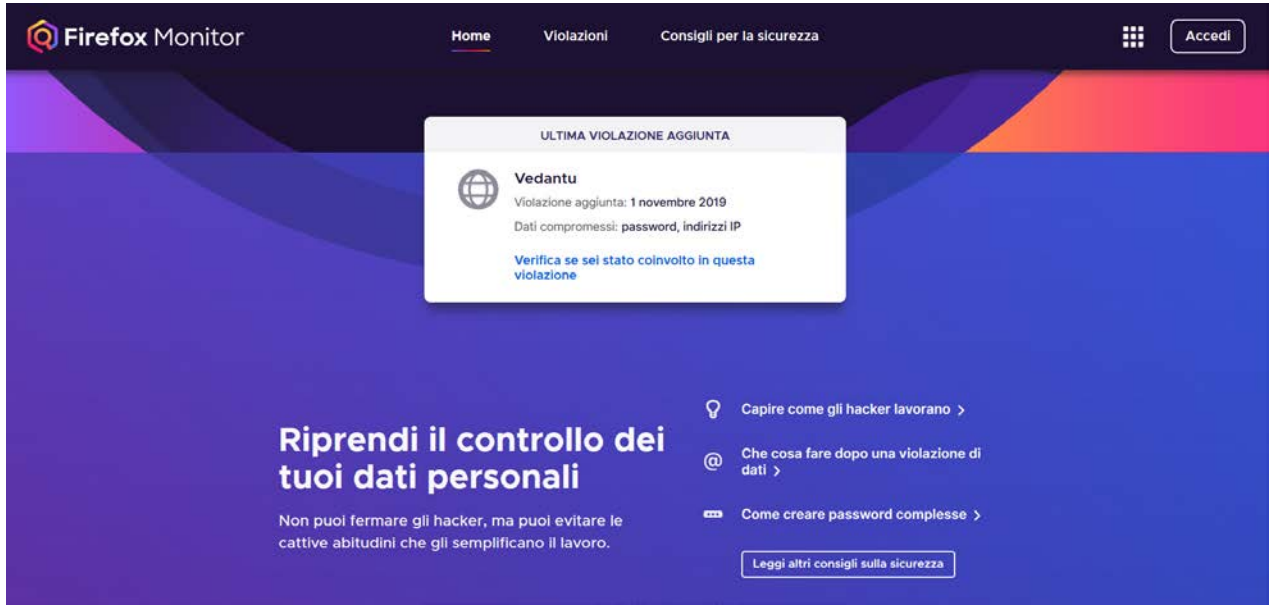
- **haveibeenpwned.com**





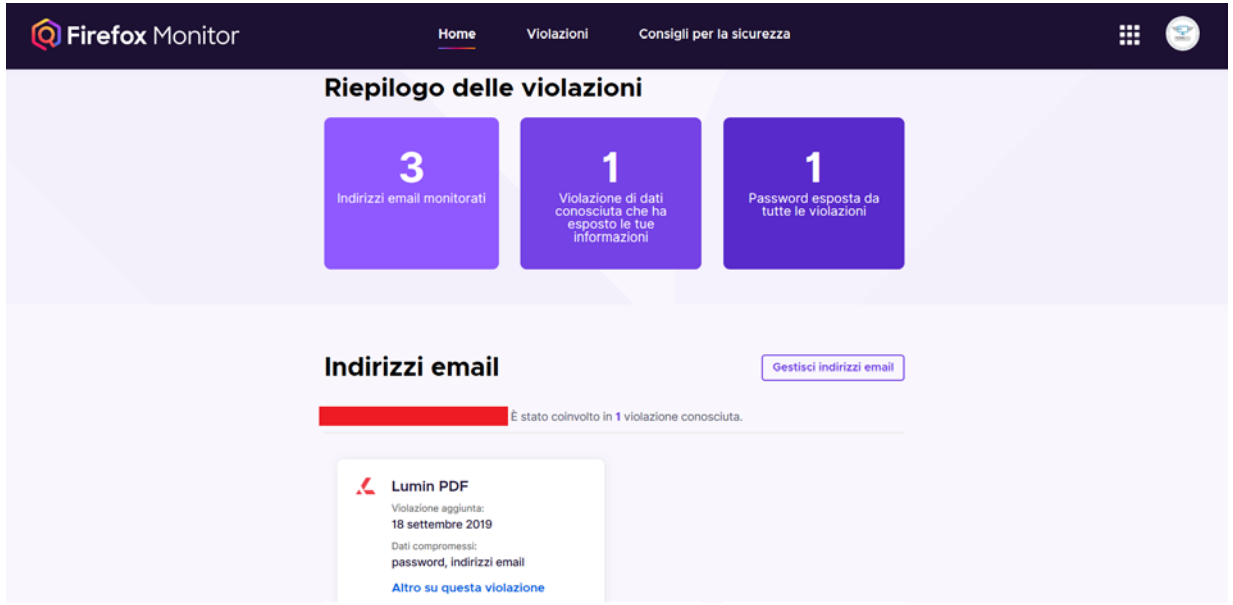
3.3 Verifica compromissione email *haveibeenpwned.com*

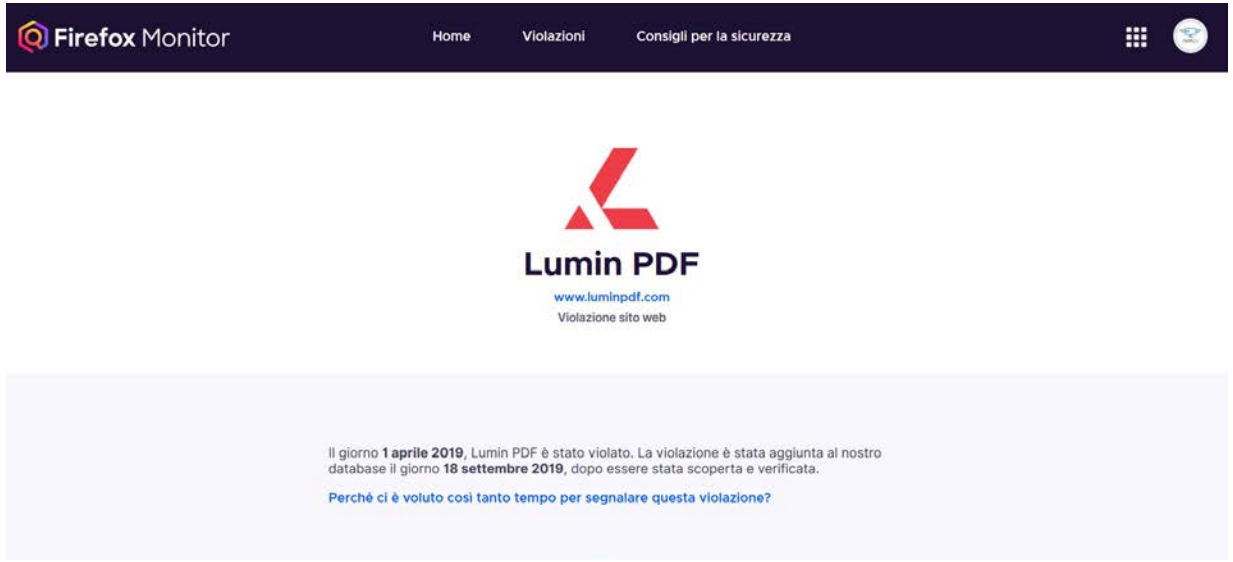
- **haveibeenpwned.com**
- **Firefox monitor** incorpora i dati del servizio **haveibeenpawned.com** per gli indirizzi immessi e verificati dall'utente
- Segnala il coinvolgimento dei propri account nei data breach mondiali non appena vengono scoperti



3.3 Verifica compromissione email

haveibeenpwned.com





3.4 Endpoint Security
Autenticazione a due fattori
(MFA, 2FA)

- **AUTENTICAZIONE A DUE FATTORI**
- metodo di autenticazione che si basa sull'utilizzo congiunto di **due metodi** di **autenticazione individuale**.
- Vengono distinti tre diversi metodi:
  - "*Una cosa che conosci*", per esempio una password o il PIN.
  - "*Una cosa che hai*", come un telefono cellulare, una carta di credito o un oggetto fisico come un token.
  - "*Una cosa che sei*", come l'impronta digitale, il timbro vocale, la retina o l'iride, o altre caratteristiche di riconoscimento attraverso caratteristiche uniche del corpo umano (biometria).
- L'**autenticazione a due o più fattori** è lo strumento principale di contrasto al **phishing** e, più in generale, a furto di credenziali.

3.4 Autenticazione a due fattori

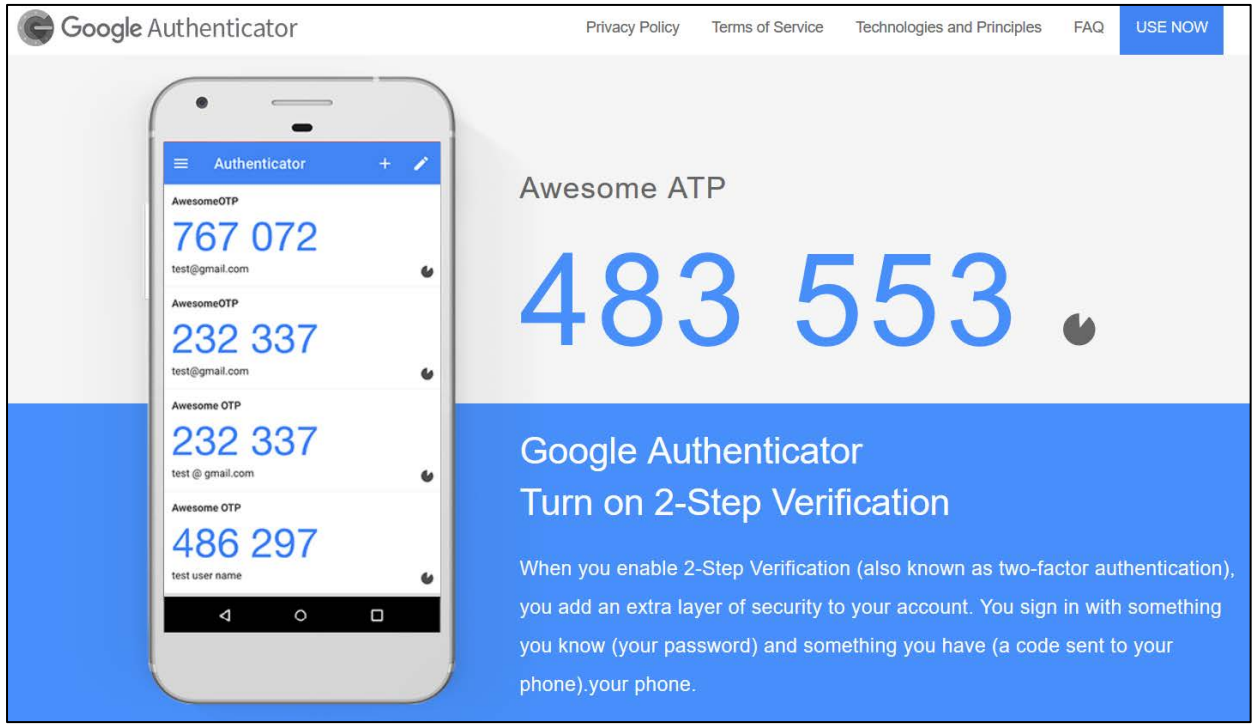
Google Authenticator

- **GOOGLE AUTHENTICATOR**
- Applicativo per la generazione **codici** realizzato da **Google** e distribuito come applicazione mobile per **Android**, **iOS** e **BlackBerry OS**
- Genera codici numerici *pseudocasuali* a intervalli regolari basandosi sul trascorrere del tempo ed altri fattori di identificazione univoca del dispositivo e dell'identità dell'utente (es. account associato, nr. serie smartphone etc.)
- Basato sugli algoritmi **HOTP** e **TOTP**
  - **HMAC-based One-time Password algorithm (HOTP) e Time-based One-time Password algorithm (TOTP)** forniscono un metodo di autenticazione mediante generazione di codici leggibili dall'uomo, ciascuno utilizzato per un solo tentativo di autenticazione
- Compatibile con account Google, Facebook, Microsoft, Amazon…

3.4 Autenticazione a due fattori

Google Authenticator

- **GOOGLE AUTHENTICATOR**



3.4.2 Autenticazione a due fattori

Yubikey

- **YUBIKEY**
- dispositivo di autenticazione hardware, prodotto dall'azienda **Yubico**, che permette l'uso di una password diversa ad ogni utilizzo. Genera una *one-time password* che permette agli utenti un'autenticazione sicura nei propri account.

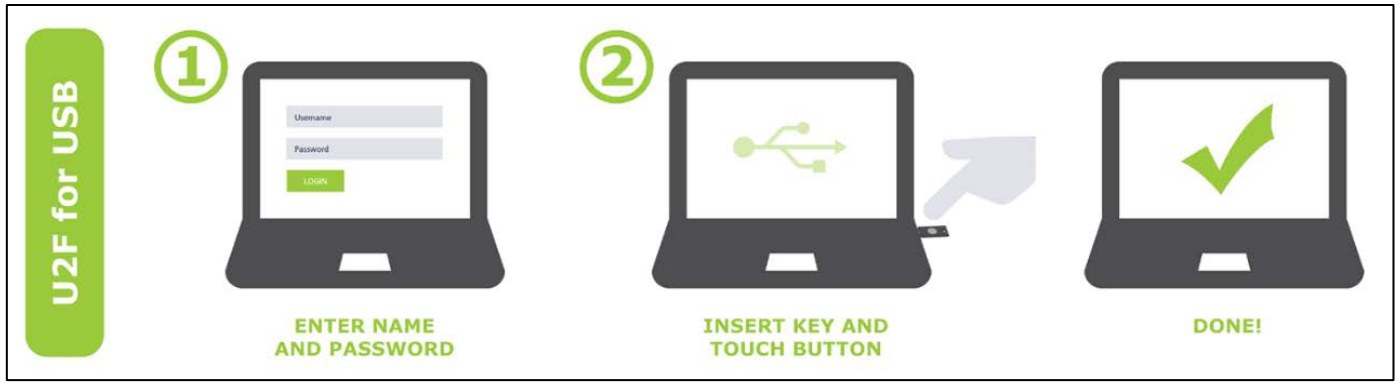
3.4.2 Autenticazione a due fattori

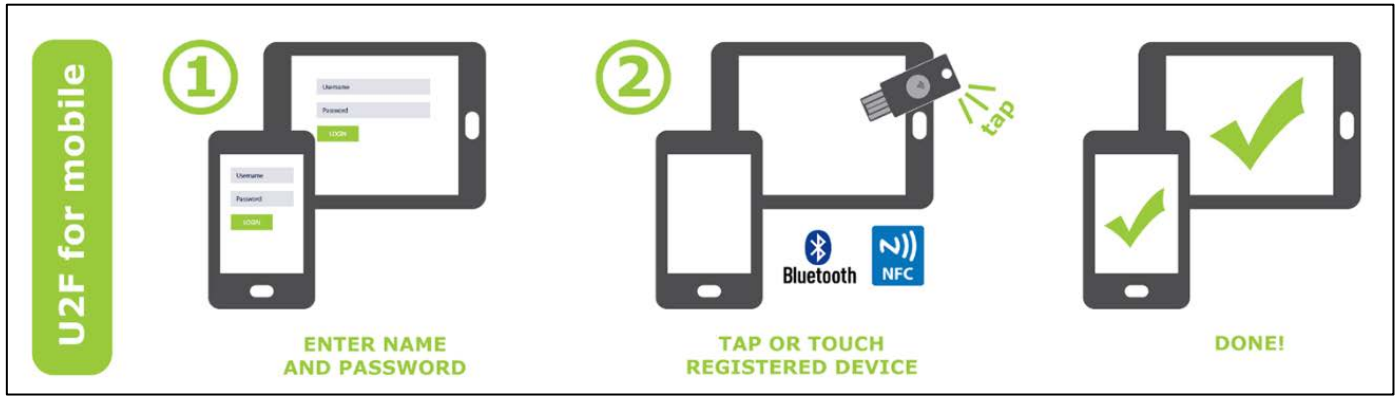
Yubikey

- Tre possibilità:
  - **Autenticazione senza password**
    - Viene utilizzato solo l'autenticatore hardware
  - **Autenticazione a due fattori**
    - L'autenticatore hardware fornisce un ulteriore livello di sicurezza oltre alla password
  - **Autenticazione multifattore**
    - Autenticazione multifattore usando l'autenticatore hardware e un PIN o un dato biometrico (es. Per le transazioni finanziarie)

3.4.2 Autenticazione a due fattori

Yubikey

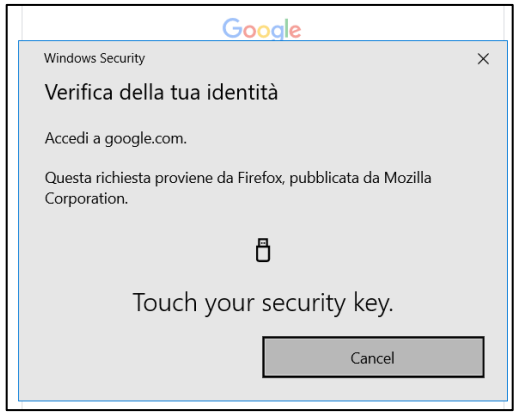


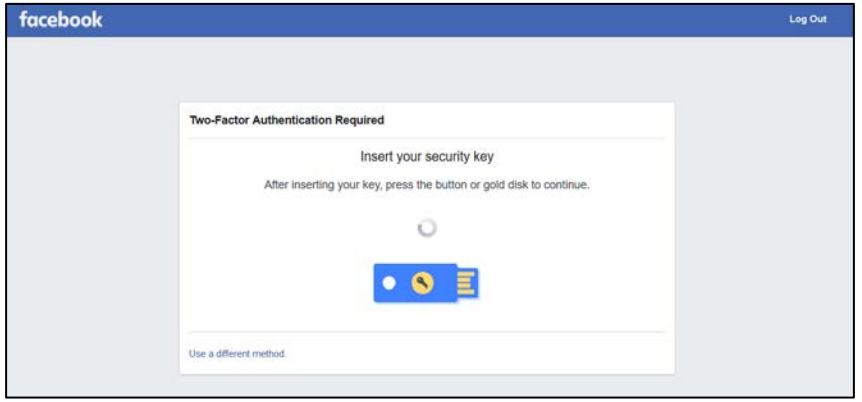


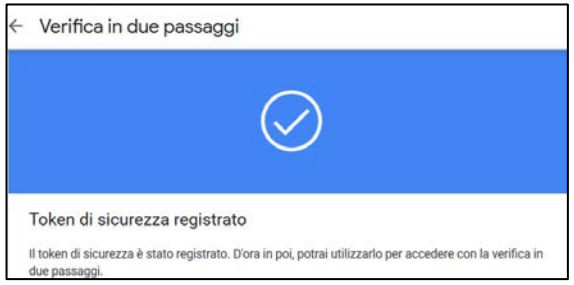
3.4.2 Autenticazione a 2 fattori

Yubikey

- **YUBIKEY**

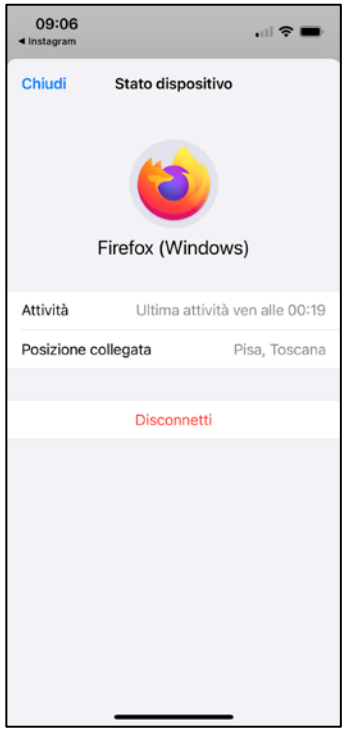






3.5 Verifica dispositivi connessi

- **Verifica dispositivi connessi**
- Le principali app di messaggistica istantanea e le app relativa a social network forniscono la possibilità di vedere i dispositivi associati agli account identificando browser web, geolocalizzazione e ultimo accesso.
- Si possono disconnettere gli accessi non riconosciuti.



4) SICUREZZA PC

4.1 Cifratura disco

- **Cifratura del disco**

- La **crittografia** o **cifratura** del disco è una tecnologia che protegge le informazioni convertendole in codice illeggibile che non può essere decifrato da persone non autorizzate

- Windows offre **Bitlocker** come servizio di cifratura nelle versioni di **Windows 10 Pro** o **Enterprise**

4.4.1 Cifratura disco
Soluzioni Windows
Bitlocker

- **Bitlocker**

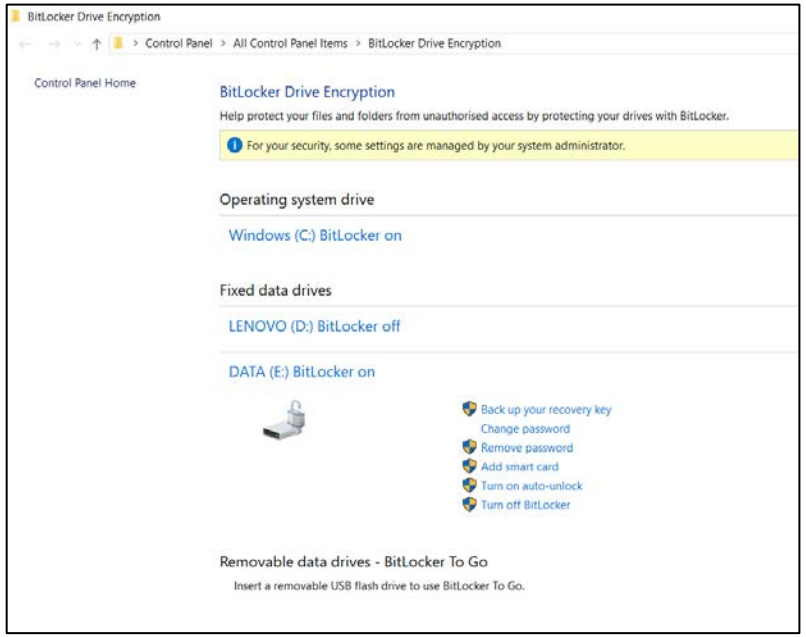
- La **BitLocker Drive Encryption** è una funzionalità di protezione dei dati integrata nei sistemi operativi Microsoft da Windows Vista e successivi che permette di crittografare l'intera partizione del sistema operativo.

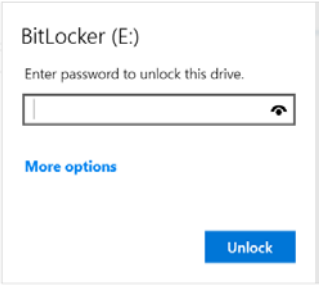
- **BitLocker** è incluso nelle edizioni **Enterprise** ed Ultimate di Vista, nelle versioni Enterprise ed **Ultimate** di **Windows 7** e nelle versioni Pro ed Enterprise di **Windows 8**, **8.1** e **Windows 10**, unitamente alle corrispondenti versioni di Windows Server.

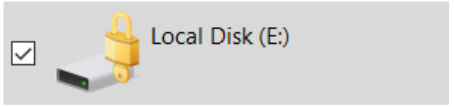
- Per impostazione di default viene usato l'algoritmo di crittografia **AES** nella modalità **CBC** (*Chypher Block Chaining*) con una chiave di **128 bit**.

4.1.1 Cifratura disco
Soluzioni Windows
Bitlocker

- Permette di stampare una recovery key da conservare separatamente e utilizzare in caso di emergenza
- Supporta lo sblocco tramite smart card
- Tramite l'applicazione **Bitlocker To Go** supporta lo sblocco tramite pendrive USB
- *Pannello di Controllo → Sistema e Sicurezza → Bitlocker*

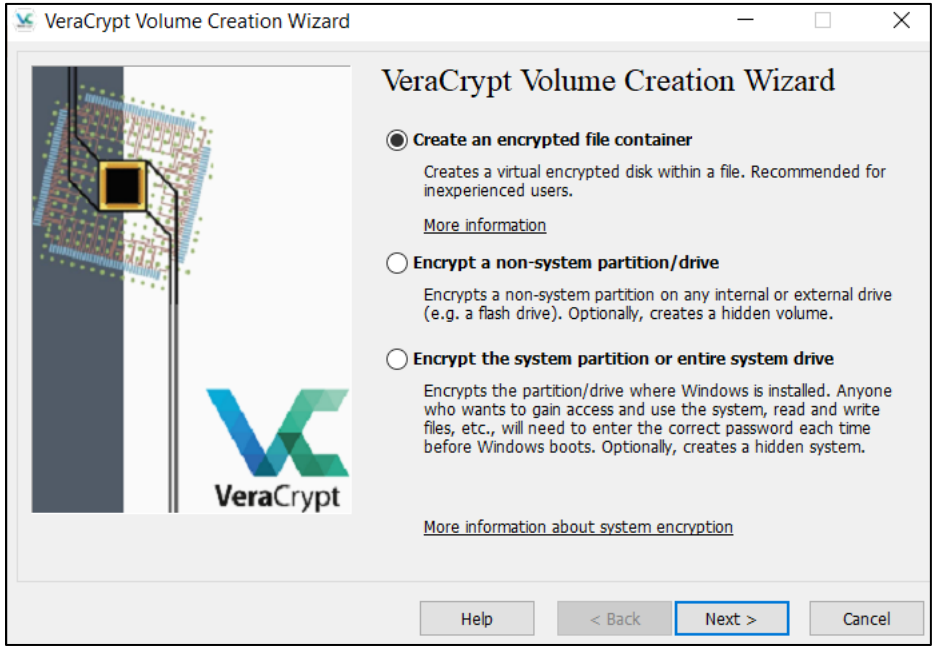






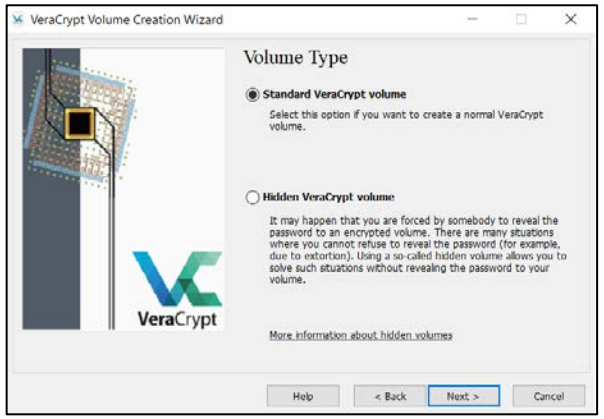
4.1.2 Cifratura disco
Soluzioni Software
Veracrypt

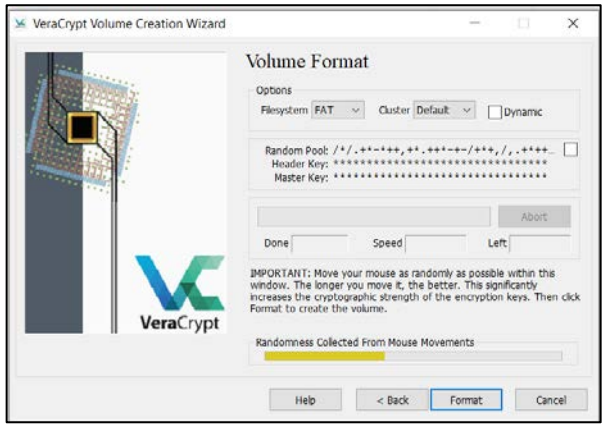
- **Veracrypt**
- Tre opzioni:
  - Creazione un disco virtuale crittografato mediante l'utilizzo di un file
  - Cifratura di partizione non di sistema
  - Cifratura completa dell'hard disk con un'autenticazione all'avvio.

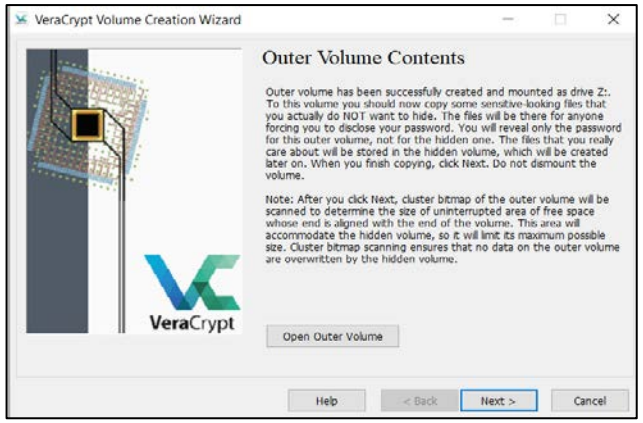


4.1.2 Cifratura disco
Soluzioni Software
Veracrypt

- **Veracrypt**
- L'opzione **ecnrypted file container** permette di creare una partizione nascosta all'interno del disco virtuale cifrato.

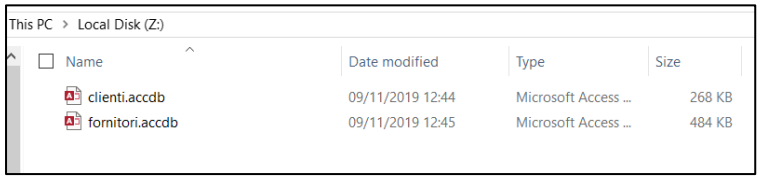


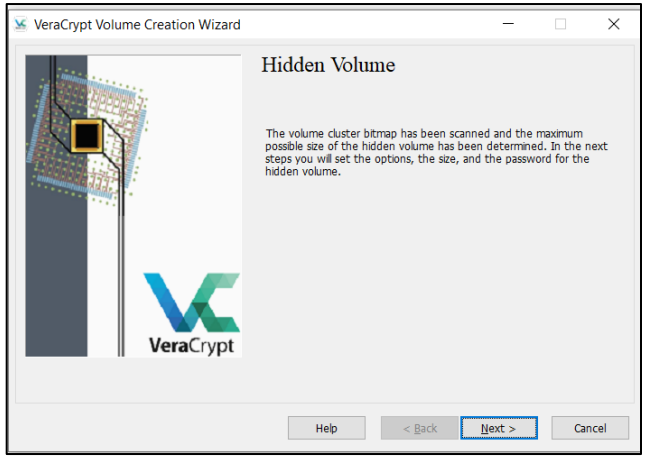


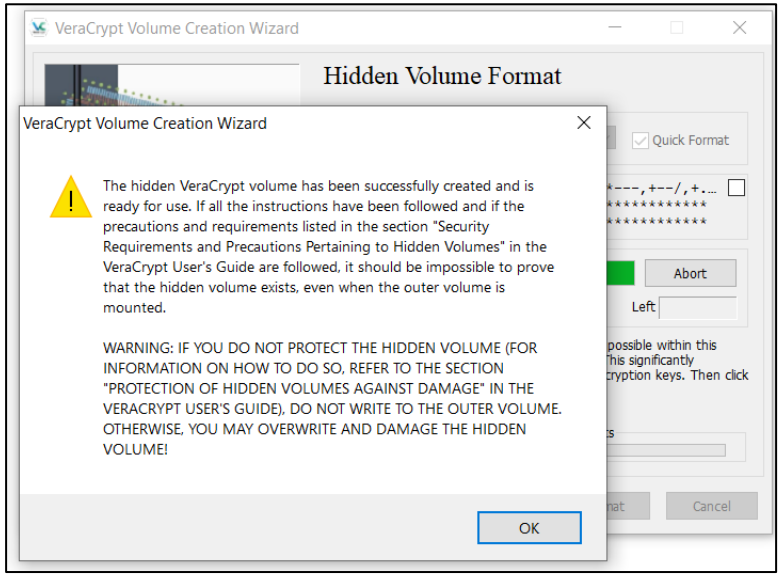


4.1.2 Cifratura disco
Soluzioni Software
Veracrypt

- **Veracrypt**

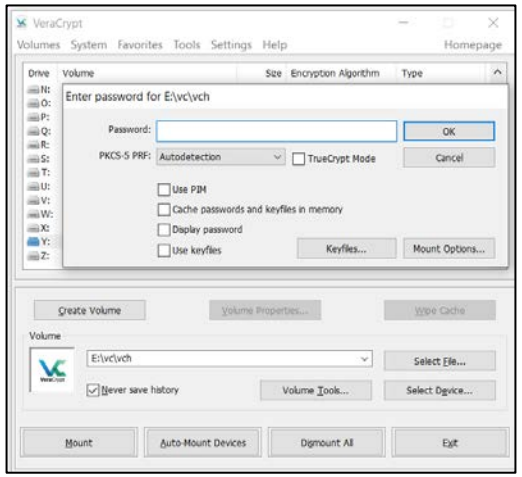


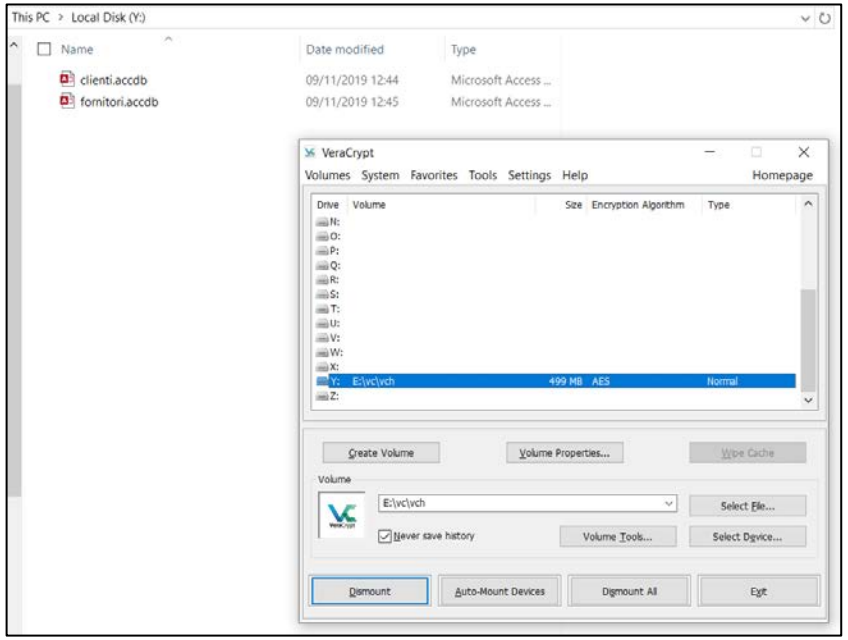


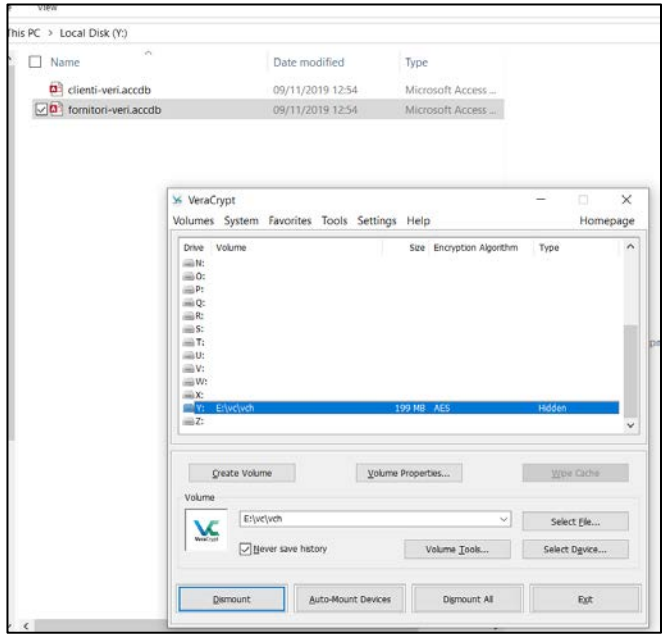


4.1.2 Cifratura disco
Soluzioni Software
Veracrypt

- **Veracrypt**







4.2 Cifrare le memorie rimuovibili

- **Perché cifrare hard disk e pendrive USB?**
- Dimensioni ridotte
- Facili da rubare
- Facili da smarrire

4.2 Cifrare le memorie rimuovibili

- **Perché cifrare hard-disk e pendrive USB?**
- Un altro buon motivo.

LA NAZIONE PISA

CRONACA SPORT COSA FARE EDIZIONI PRECIPITA DAL BALCONE TRAFFICO FIRENZE TERREMOTO LA MORTE DI HELENIA

HOME › PISA › CRONACA Pubblicato il 16 aprile 2019

Sesso estremo con i ferri chirurgici. Condannato medico dell'ospedale

Scoperto per una chiavetta con le foto hard dimenticata nel camice

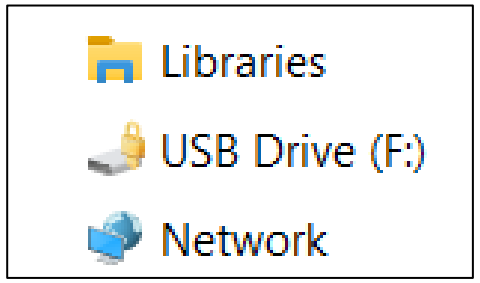
Ultimo aggiornamento il 16 aprile 2019 alle 09:26

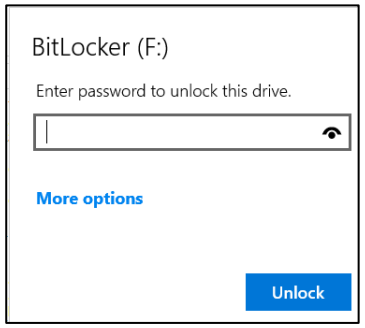
in giudizio) per 3mila 500 euro oltre accessori di legge. Tutto cominciò, nel 2014, quando l'addetto di una **lavanderia di Ponsacco trovò, in un camice, una penna usb.** L'uomo raccontò di aver curiosato fra i contenuti della chiavetta per risalire al proprietario del piccolo archivio digitale che conteneva scatti provatissimi. Scatti anche a sfondo sessuale e dove degli strumenti chirugici sarebbero stati ultilizzati per giochi erotici anche a bordo di un mezzo a Collesalvetti, oltre che per le normali attività ambulatoriali.

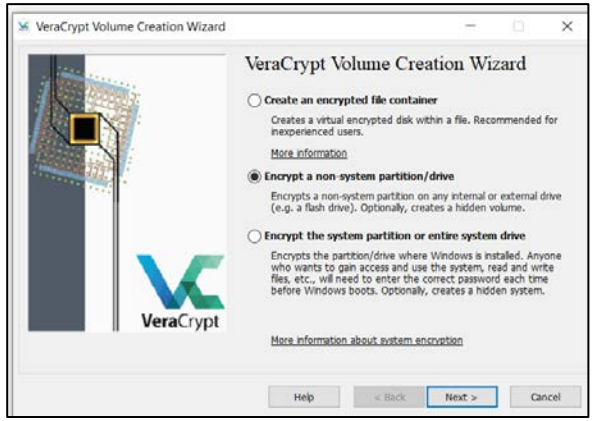
4.2.1 Cifrare le memorie rimuovibili

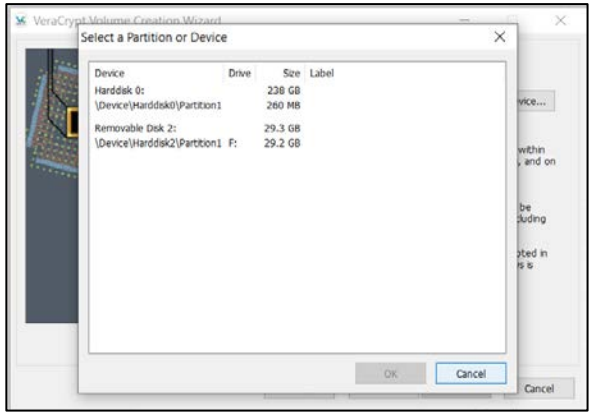
Bitlocker, Veracrypt

- **Bitlocker, Veracrypt**
- Entrambi isoftware visti in precedenza supportano la cifratura dei dispositivi rimuovibili.







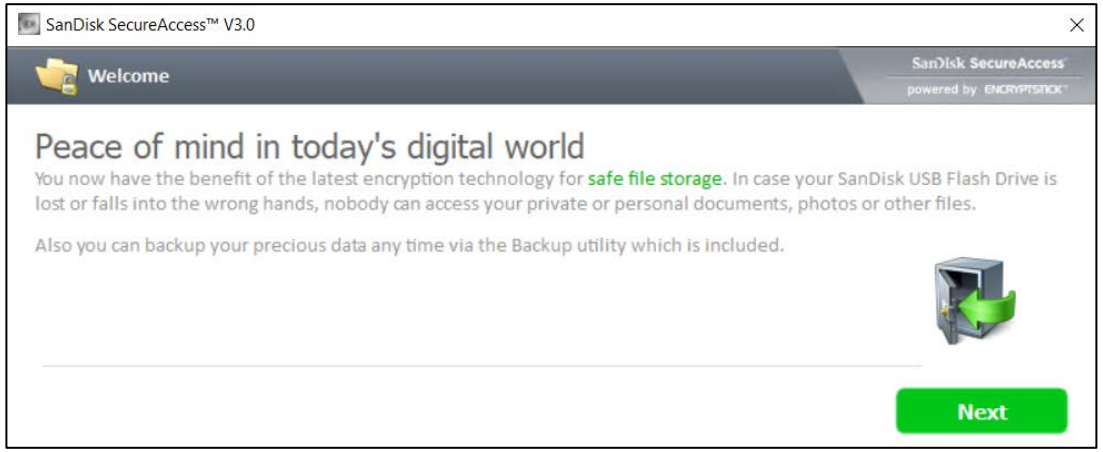


- Unico limite: il software deve essere presente anche sul computer su cui si vogliono connettere le memorie USB.

4.2.2 Cifrare le memorie rimuovibili

Software di cifratura *SanDisk Secure Access*

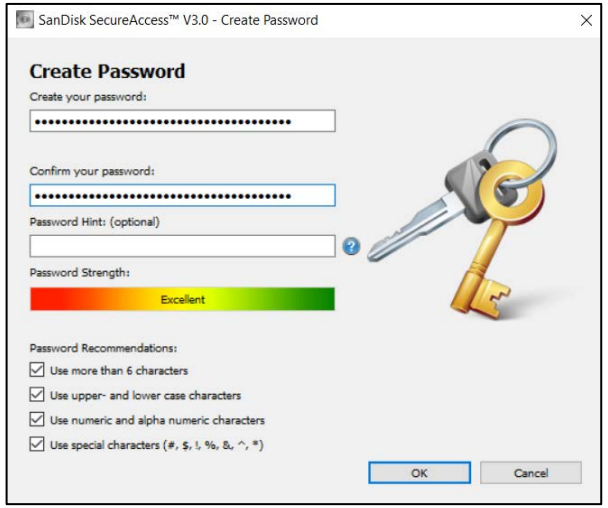
- **SanDisk Secure Access**
- Software di cifratura presente sui dispositivi rimuovibili **SanDisk**

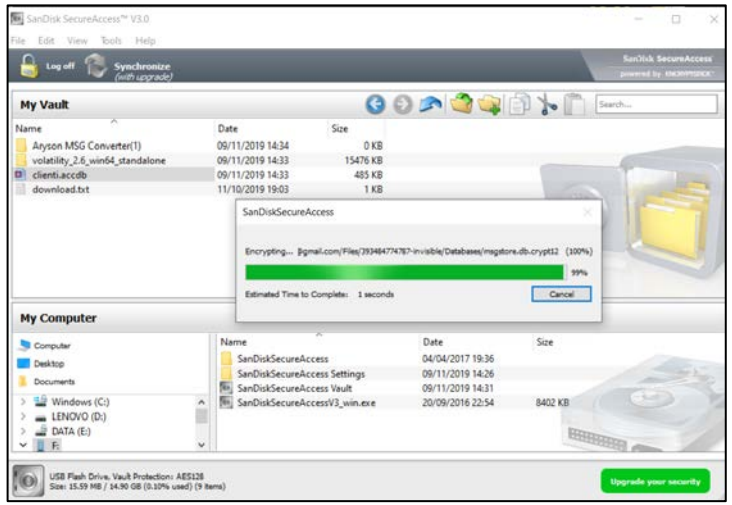


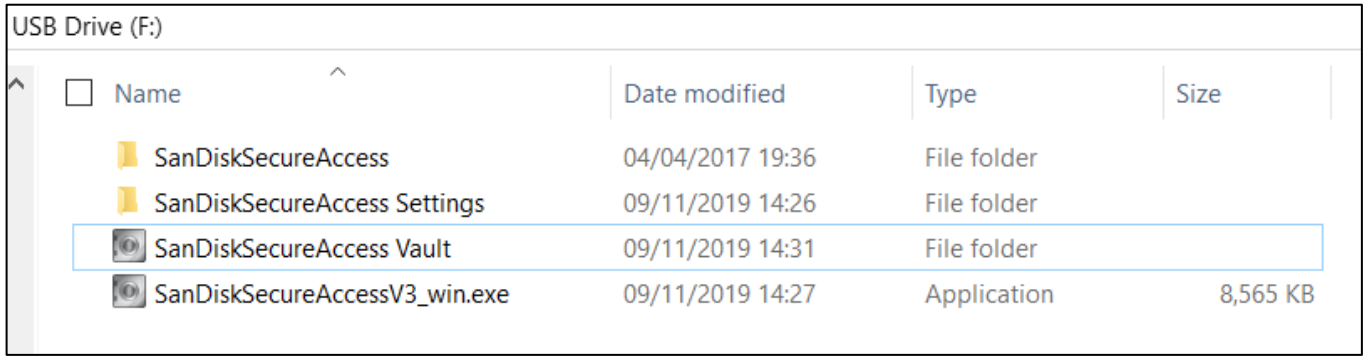
4.2.2 Cifrare le memorie rimuovibili

Software di cifratura *SanDisk Secure Access*

- **SanDisk Secure Access**







4.2.3 Cifrare le memorie rimuovibili

Cifratura integrata su Cloud

Kingston Data Traveler Locker

- **Kingston Data Traveler Locker**

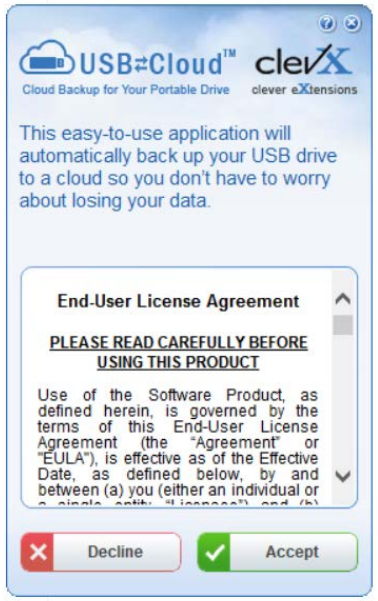
- Software integrato nella pendrive che permette la sincronizzazione su Cloud
- L'unità viene bloccata e formattata dopo 10 tentativi di accesso falliti
- Assemblata con guscio in metallo di protezione

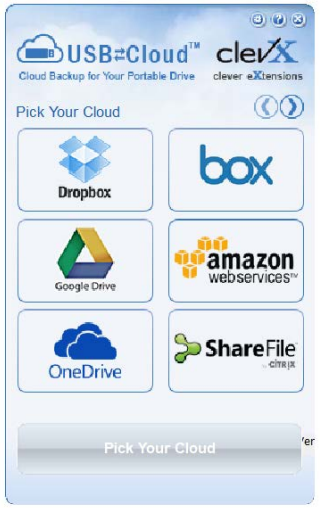
4.2.3 Cifrare le memorie rimuovibili

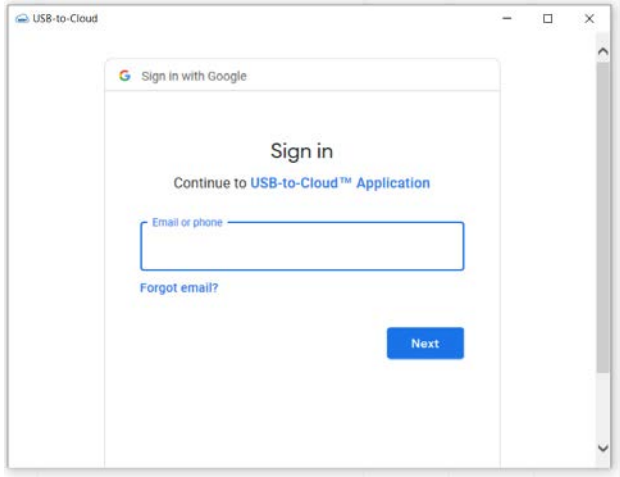
Cifratura integrata su Cloud

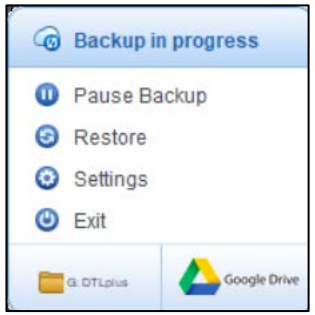
Kingston Data Traveler Locker

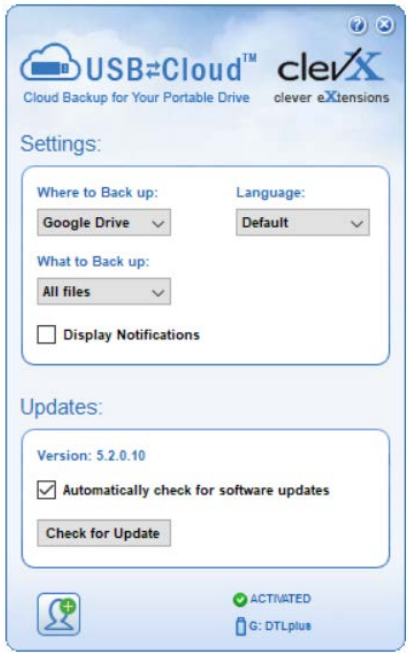
- **Kingston Data Traveler Locker**











4.2.4 Cifrare le memorie rimuovibili
PIN a immissione fisica
Lepin KP001

- **Lepin KP001**

- Cifrata a livello hardware
- Immissione di PIN tramite *keypad* sulla superficie della pendrive
- PIN 6-14 cifre (numeri da 0-9)
- Assemblata con guscio in alluminio zincato
- Ogni dispositivo ha un **codice identificativo univoco** da inviare al produttore per ricevere una chiave a 10 bit di emergenza da utilizzare per lo sblocco.

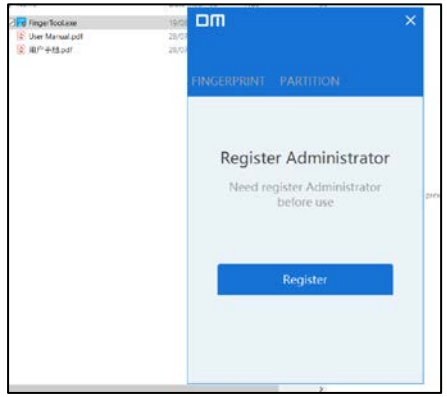
4.2.4 Cifrare le memorie rimuovibili

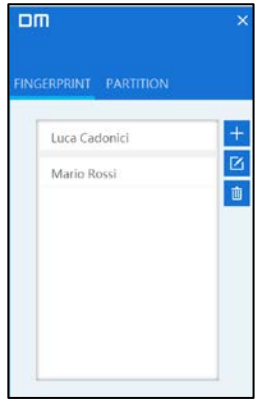
Pendrive con sblocco biometrico

Forrader Fingerprint

- **Forrader Fingerprint**

- Sblocco biometrico tramite impronta digitale
- Supporta fino a 6 impronte digitali:
  - 1 **amministratore**
  - 5 **utenti**
- L'amministratore può **aggiungere nuove impronte**, **partizionare la memoria** tra spazio **segreto** e **pubblico**, nonché rimuovere gli utenti





4.3 Cifrare le credenziali memorizzate nei browser

- Le credenziali normalmente vengono memorizzate nei browser non cifrate
- Qualsiasi utente acceda al computer può visualizzare le password memorizzate in chiara effettuando i passaggi giusti
- Questa procedura può essere velocizzata utilizzando software forensi o *password sniffer*.

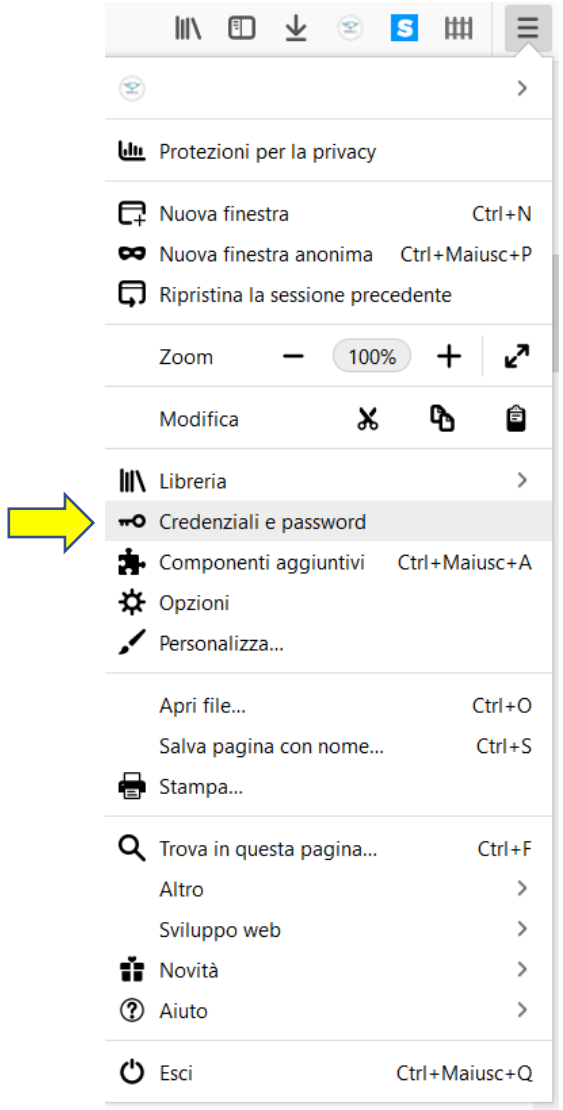
https://www.nirsoft.net/toolsdownload/webbrowserpassview.zip

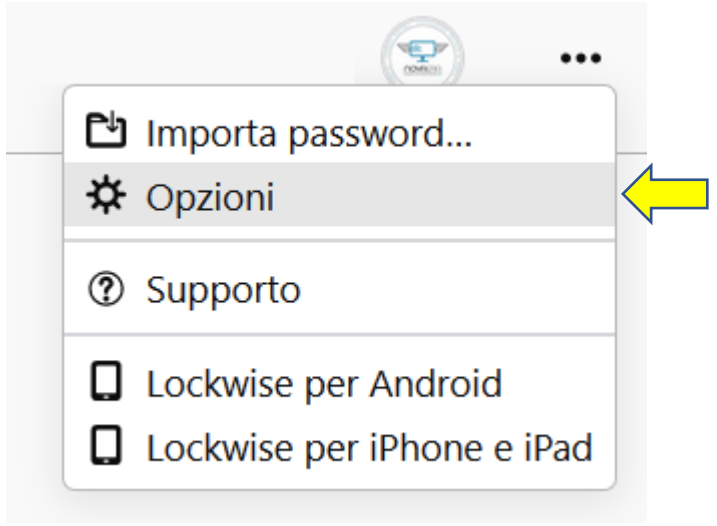
4.3 Cifrare le credenziali memorizzate nei browser

- Per impedire l'acquisizione delle credenziali memorizzate è possibile inserire una *Master Password* con cui cifrare le altre password memorizzate nel browser
- La procedura può essere effettuata anche che sul *client mail* **Thunderbird** sviluppato sempre da **Mozilla**

4.3 Cifrare le credenziali memorizzate nei browser

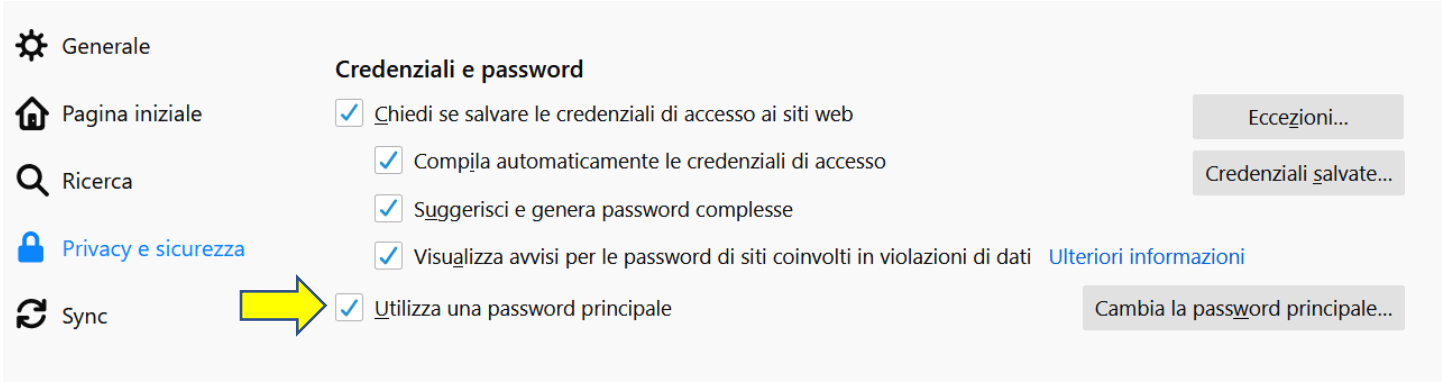
- **Firefox**

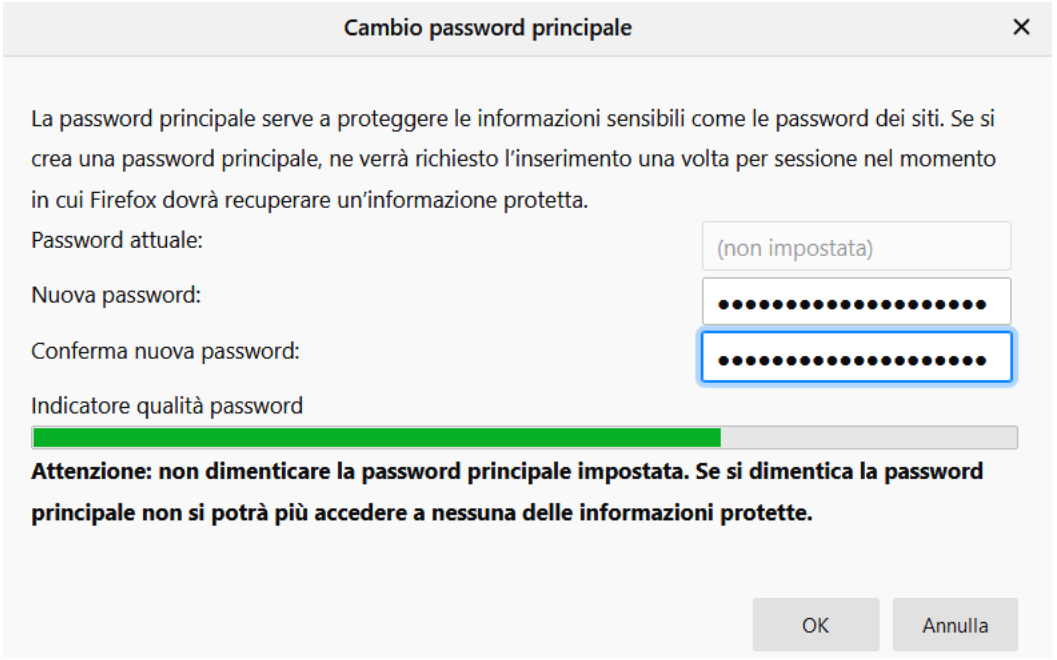




4.3 Cifrare le credenziali memorizzate nei browser

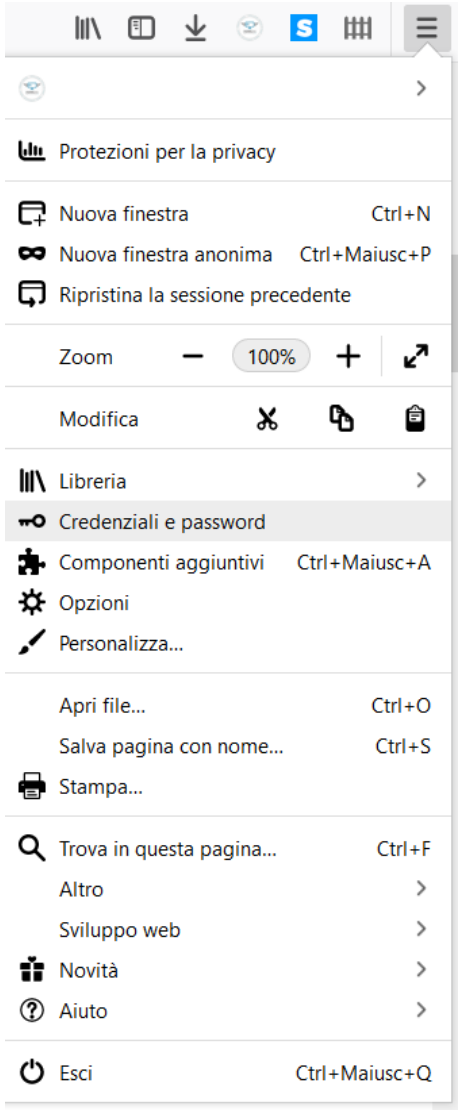
Firefox

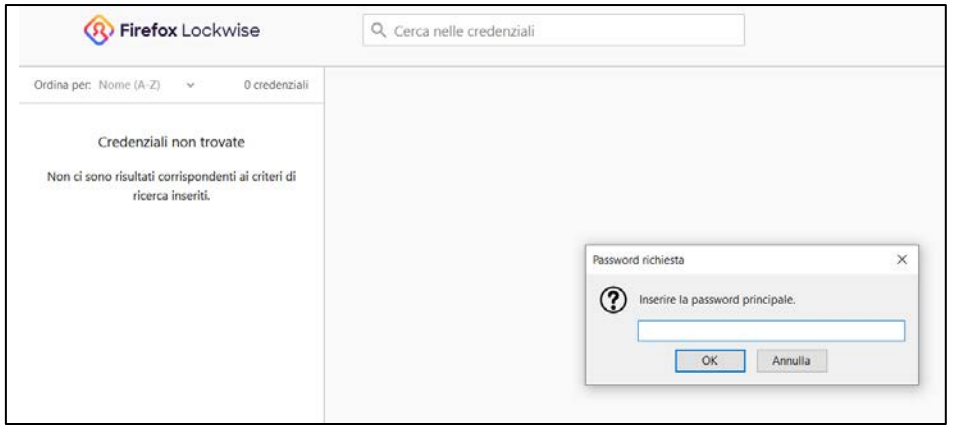




4.3 Cifrare le credenziali memorizzate nei browser

Firefox





- Le credenziali memorizzate su Firefox non vengono più acquisite

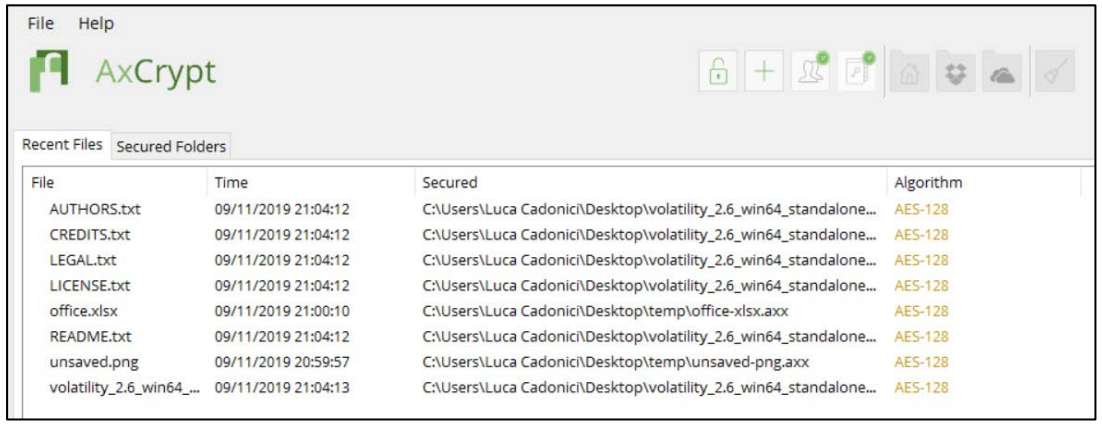
https://www.nirsoft.net/toolsdownload/webbrowserpassview.zip

4.4 Cifrare i file

AxCrypt

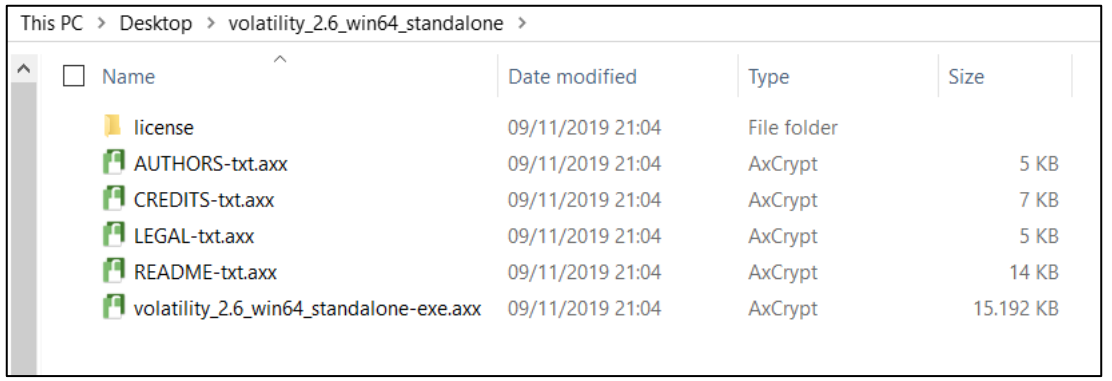
- **AxCrypt**

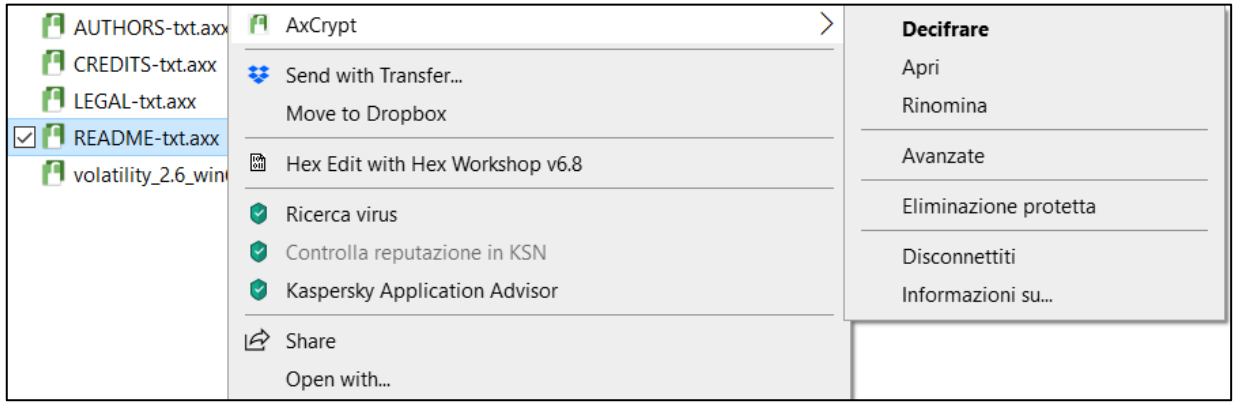
- Cifratura a livello di file
- Può cifrare file o cartelle
- Supporta **AES-128** e **AES-256**
- Necessita della creazione di un account
- Una volta effettuato il login l'utente può cifrare o decifrare i file con la propria password
- Si può utilizzare un file per cifrare un file o una cartella
- I file scambiati con utenti che utilizzano **Axcrypt** possono essere decifrati se si conosce la password
- I file vengono rinominati in **.axx**
- Compatibile con **Google Drive** o **Dropbox**



4.4 Cifrare i file
AxCrypt

- **Cifrare una cartella**
- La struttura gerarchica viene mantenuta
- I file presenti in essa vengono rinominati in .axx

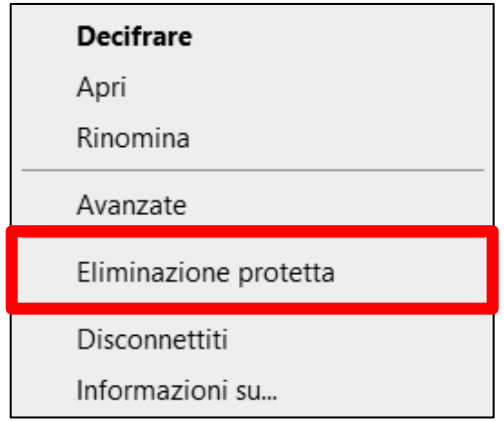




4.5 Eliminazione sicura dei file

AxCrypt

- **Eliminazione protetta dei file**
- Nel file-system NTFS tipico di Windows i file cancellati non sono immediatamente rimossi dal sistema ma solamente resi inaccessibili agli utenti
- Normalmente i file cancellati di recente sono quindi recuperabili con software apposito
- **AxCrypt** supporta la funzione di eliminazione protetta: scompone i file prima di cancellarli in modo che non siano più recuperabili.
- L'obiettivo è renderli irrecuperabili a utenti malintenzionati



4.6 Pulizia spazio non allocato e cronologica d'uso *CCleaner*

- **Pulizia spazio non allocato**

- ***Spazio non allocato***
  - *Cluster* di una partizione multimediale non in uso per la memorizzazione di file attivi. Possono contenere frammenti di file che sono stati eliminati dalla partizione di file ma non rimossi dal disco fisico.
- ***Slack space***
  - Lo spazio inutilizzato alla fine di un file in un *file-system* che utilizza cluster di dimensioni fisse. Se il file è di dimensione inferiore al *cluster*, lo spazio inutilizzato non viene modificato e può contenere tracce di dati precedentemente memorizzati
  - In NTFS i *cluster* sono usualmente di 4Kb.

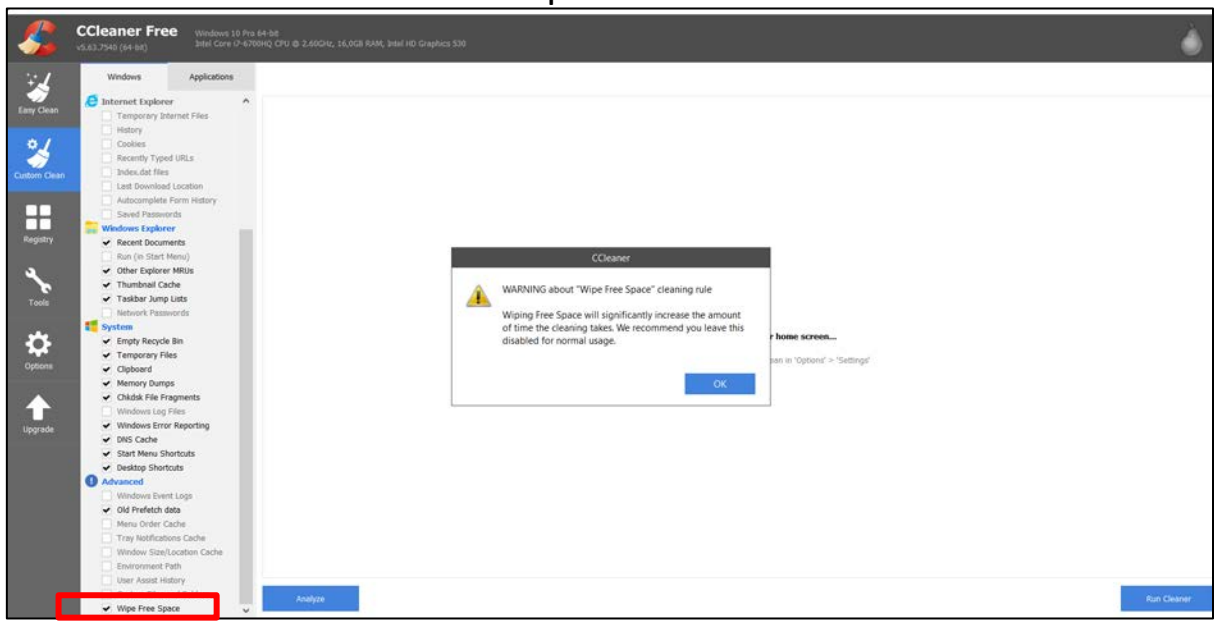
- I dati ancora presenti possono essere usati per recuperare password e altri dati di accesso, parti di file, comunicazioni

4.6 Pulizia spazio non allocato e cronologica d'uso *CCleaner*

- **Pulizia spazio non allocato**

I dati cancellati ma ancora fisicamente presenti possono essere usati per recuperare password e altri dati di accesso, parti di file, comunicazioni

- ***CCleaner***
  - **CCleaner** è un software *freeware* che permette l'**ottimizzazione delle prestazioni**, la **protezione della privacy,** la **pulizia del registro di sistema** e altre **tracce d'uso (dati recenti, cronologia internet, file temporanei etc.)**
  - Principalmente elimina i **dati temporanei** prodotti dall'uso dell'utente
  - Supporta l'opzione ***Wipe Free Space*** che consente di cancellare le tracce di dati cancellati ancora presenti



4.11 Antivirus

- **Antivirus**
  - *Kaspersky*
  - *Sophos*
  - *Bitdefender*
  - *Norton*
  - *TrendMicro*
  - *Eset*

- **Investite un piccolo budget in un antivirus professionale e non gratuito in modo da innalzare significativamente il vostro livello di sicurezza**

4.13 Patching e aggiornamenti

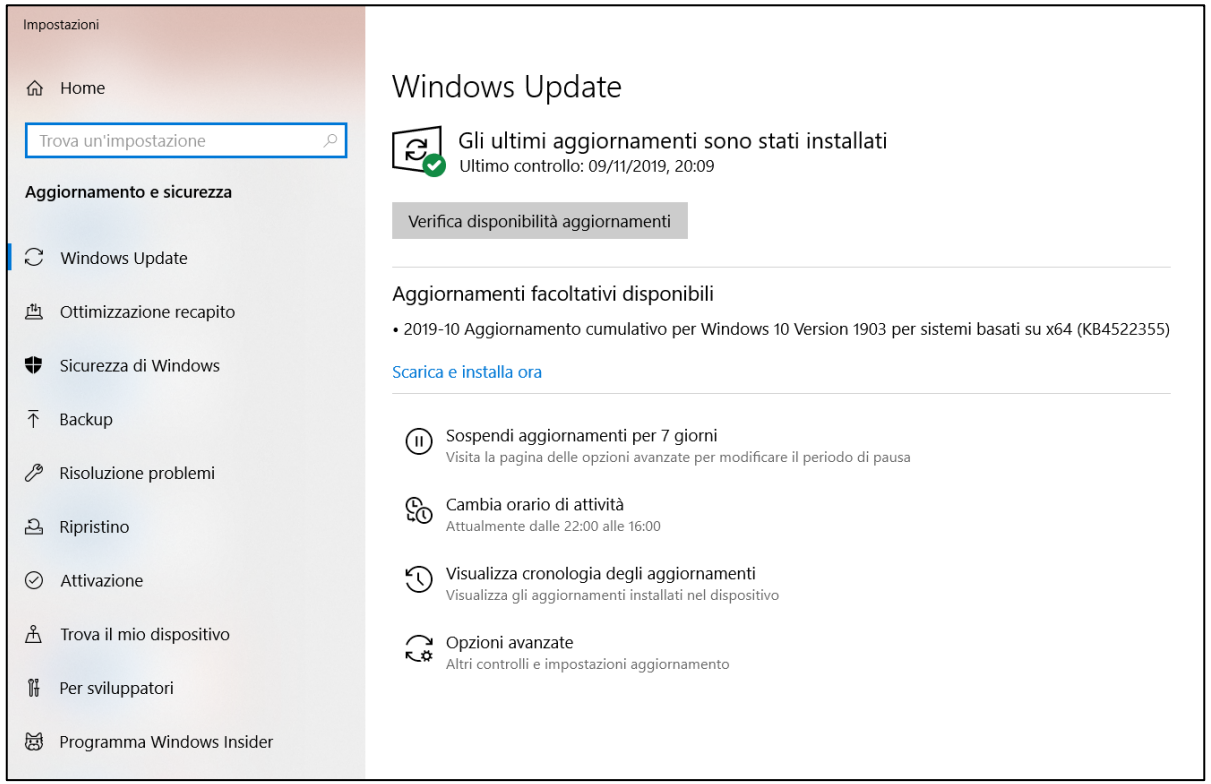
- **Patching**
- Una **patch** di sicurezza è un aggiornamento finalizzato alla correzione di vulnerabilità.
- Le **patch** di sicurezza sono il sistema primario di correzione delle vulnerabilità software.
- Per i sistemi operativi vi sono team specializzati nello sviluppo e nella pubblicazione di **patch** di sicurezza, i quali periodicamente le pubblicano.

- Due tipologie:
  - Patch del Sistema Operativo
  - Patch delle applicazioni di terze parti

4.8.1 Patching
Patch di Windows
Windows Update

- **Patch di Windows**

- Controllare che **Windows Update** sia attivato
- Controllare che gli **aggiornamenti di Windows** siano stati installati

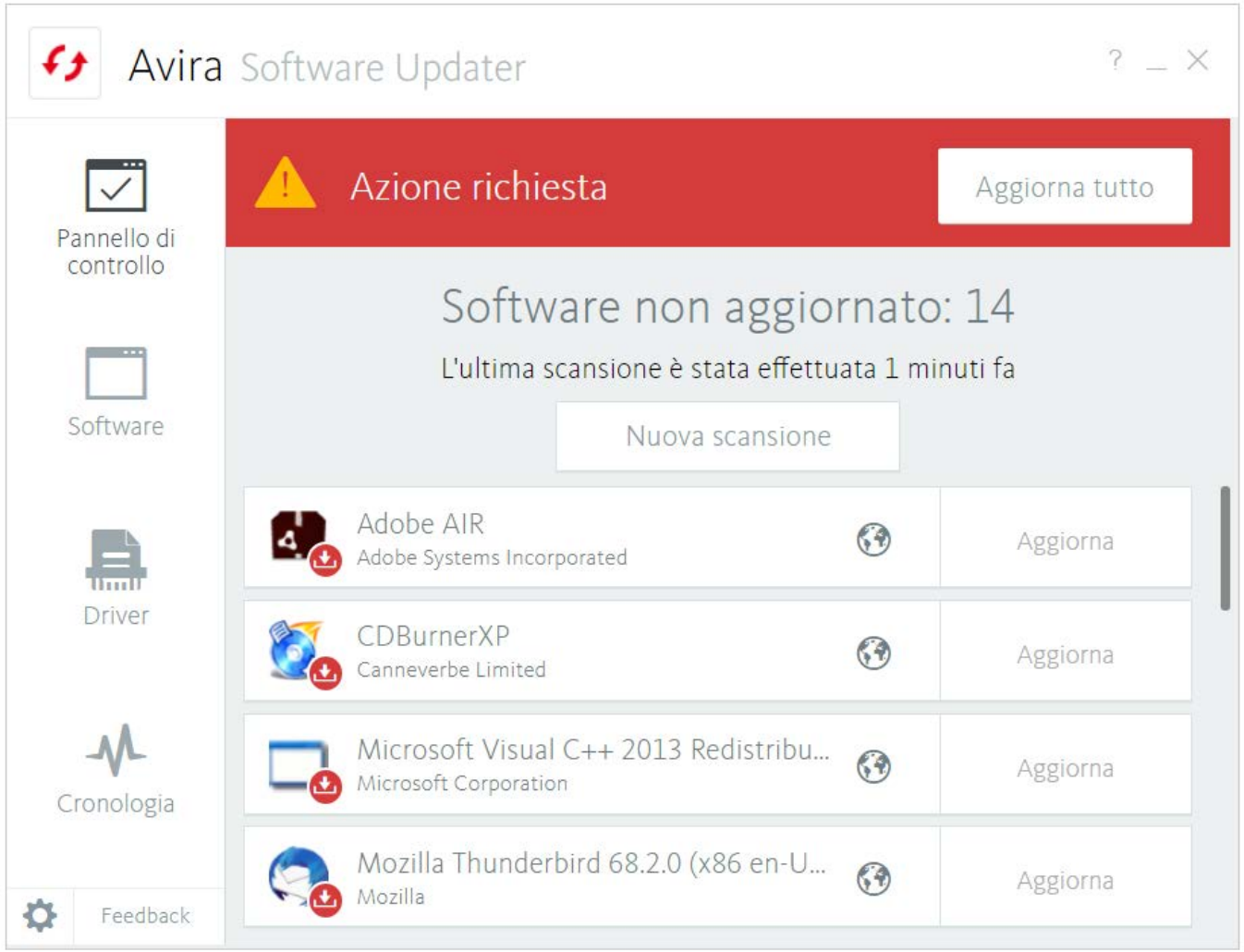


4.13 Patching e aggiornamenti

Patch per applicazioni di terze parti

Avira Software Updater

- **Patch applicazioni**
- **Avira Software Updater**



5) NAVIGARE IN SICUREZZA

5. Navigare in sicurezza
Protezione da phishing e malware

- **Sito web ingannevole o di *phishing*:** cerca di presentarsi come il sito originale e legittimo al fine di indurre l'utente a fornire informazioni personali e dati sensibili come le password, i dettagli dell'account o i numeri della carta di credito.
- Gli attacchi di *phishing* solitamente provengono da messaggi email che cercano di invitare il destinatario ad aggiornare i propri dati personali su siti web falsi ma molto simili ai siti legittimi

- **Sito web malevolo:** progettato in modo da infettare il computer con software malevolo (*malware*) quando lo si visita.

5.1 Navigare in sicurezza
Protezione da phishing e malware
Firefox

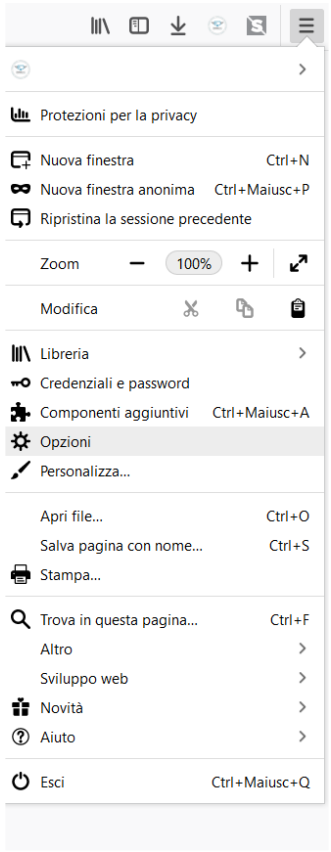
- In **Firefox** è presente una funzione per la protezione da *phishing* e *malware* integrata nel browser a salvaguardia dell'utente durante la navigazione nel Web.
- Questa caratteristica consente di visualizzare un avviso che invita a prestare molta attenzione quando si visita una pagina che è stata segnalata come **sito ingannevole**, come origine di **software indesiderato** o come **sito web malevolo** (origine di *malware*) progettato per danneggiare il computer utilizzato.
- Questa caratteristica viene anche utilizzata per segnalare la presenza di eventuali **file scaricati riconosciuti come *malware***

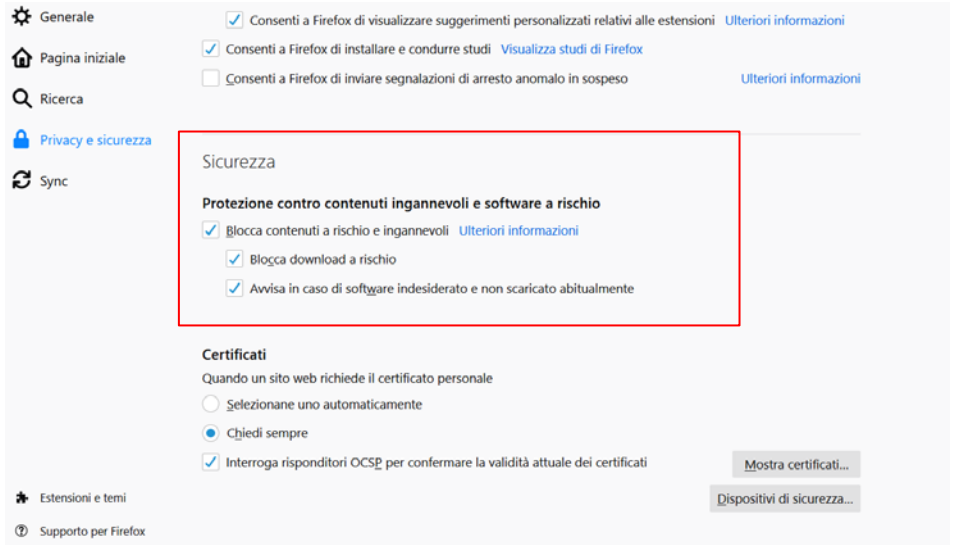
5.1 Navigare in sicurezza
Protezione da phishing e malware
Firefox

- La protezione da phishing e malware funziona controllando i siti visitati dall'utente e mettendoli a confronto con i siti *phishing*, software indesiderato e malware segnalati come tali e contenuti in speciali elenchi organizzati da associazioni non-profit specializzate e da *Google*.
- Alcuni esempi:
  - **Anti-Phishing Working Group** - https://apwg.org/
  - **Google Safe Browsing** - https://safebrowsing.google.com/safebrowsing/report_phish/?hl=it
  - **StopBadware** - https://www.stopbadware.org

5.1 Navigare in sicurezza
Protezione da phishing e malware
Firefox

- **Firefox**





6) SICUREZZA WI-FI

6. Sicurezza Wi-Fi

- **Wi-Fi**
- Tecnologia per reti locali senza fili (WLAN) che utilizza dispositivi basati sugli standard **IEEE 802.11**
- Dispositivi compatibili Wi-Fi possono connettersi a Internet tramite una WLAN e un punto di accesso wireless (**access point**).
- **WLAN:** reti locali di computer che non utilizzano dei collegamenti via cavo per connettere fra loro gli host della rete.

IEEE (*Institute of Electrical and Electronic Engineers*): associazione internazionale di scienziati per la promozione delle scienze tecnologiche

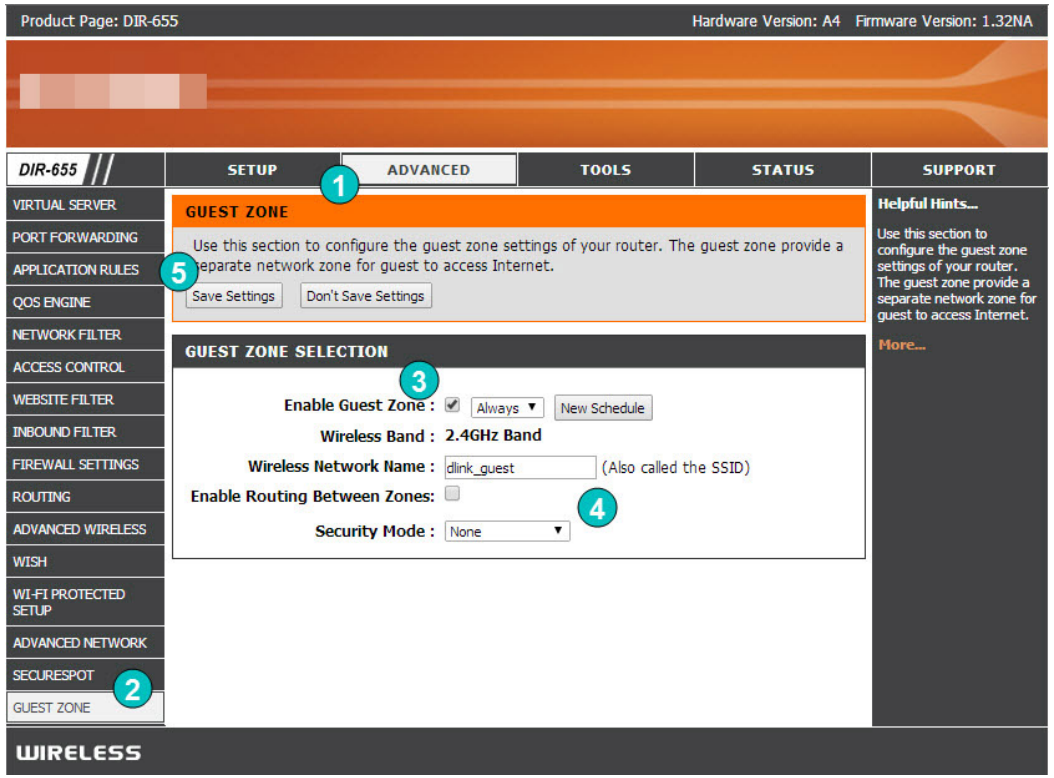
6.1 Sicurezza Wi-Fi

Sniffing

- **Sniffing**
- Attività di intercettazione passiva dei dati che transitano in una rete telematica.
- Permette di catturare e analizzare tutti i dati che passano all'interno di una rete wireless
- **CONTROMISURE:** Protocolli di sicurezza wireless che permettono la cifratura dei dati trasmessi dalle onde radio con un **sufficiente livello di sicurezza**
  - **WEP: deprecato** (due chiavi a 40 e 104 bit)
  - Usare **WPA e WPA2**: chiavi a 128bit

6.2 Sicurezza Wi-Fi
Separazione delle reti

- **Separazione delle reti**
- Creare una rete **guest** per gli ospiti presenti in a casa o a lavoro.
- Si può fare tramite accesso diretto al router wi-fi tramite browser web



7) MOBILE SECURITY

7 Mobile Security

Mobile Security

- Crescita esponenziale del numero di dispositivi mobili
- Dispositivi sempre più performanti e connessi
- Crescita esponenziale delle *app* (applicazioni mobili)

- **Rischi per la sicurezza**:
  - presenza di malware
  - accesso non autorizzato a dati personali
  - utilizzo intensivo delle risorse
  - spyware
  - smarrimento dei dispositivi

7.1 Mobile Security
Codici di sblocco

Codici di sblocco

- Prima misura di sicurezza

- Tipologia varia:
  - Sequenza di numeri
  - Sequenza grafica
  - Password
  - Dati biometrici (impronta digitale/Face ID)

  - **<u>Attivare sempre la protezione offerta dal codice di sblocco</u>**.
  - L'attivazione del codice di sblocco produce una chiave aggiuntiva utilizzata per le decifratura dei dati utente
  - Prediligere PIN alle sequenze grafiche (entropia maggiore, minore vulnerabilità allo *shoulder surfing*)

7.1 Mobile Security
Codici di sblocco

- **Codici di sblocco**
- Evitare PIN e sequenze comuni

	PIN
#1	1234
#2	1111
#3	0000
#4	1212
#5	7777
#6	1004
#7	2000
#8	4444
#9	2222
#10	6969
#11	9999
#12	3333
#13	5555
#14	6666
#15	1122
#16	1313
#17	8888
#18	4321
#19	2001
#20	1010

1	123456
2	111111
3	123123
4	000000
5	321654
6	123321
7	520131
8	520520
9	112233
10	147258

7.2.1 Mobile Security
Cifratura dei dati

Cifratura dei dati

- La cifratura è il processo di codifica di tutti i dati utente presenti sul dispositivo utilizzando una combinazioni di chiavi hardware (ovvero inscritte nel dispositivo) e derivate dal codice di sblocco impostato dall'utente.

- Una volta crittografato un dispositivo, tutti i dati creati dall'utente vengono crittografati automaticamente prima di essere scritti su disco e decifrati ogni volta che vengono richiesti dall'utente

- La cifratura garantisce l'inintellegibilità dei dati ad un utente non autorizzato, ovvero diverso dal possessore del dispositivo.

7.2.1 Mobile Security Cifratura dei dati iOS

- **Cifratura dei dati**
- **Apple**
  - Apple ha introdotto la crittografia nel 2014 con i primi dispositivi dotati di iOS 8.
  - Ogni dispositivo ha una chiave immutabile di 256-bit unica chiamata **UID**, che viene generata in modo casuale e fusa nell'hardware del dispositivo quando viene prodotto.
  - Questa password viene poi combinata con il codice di sblocco impostato dall'utente e associato all'autenticazione biometrica (*Face ID* o *Touch ID*).

7.2.1 Mobile Security Cifratura dei dati iOS

Cifratura dei dati

- I dati considerati più sensibili (es. *Salute*, *Portachiavi*, *Homekit*) adottano la cifratura punto-punto (*end-to-end encryption*)

- **In caso di rimozione SIM o riavvio del dispositivo l'autenticazione biometrica viene disattivata e lo sblocco è possibile solo tramite il PIN**.

7.2.1 Mobile Security Cifratura dei dati iOS

- **Cifratura dei dati**
- **Apple**
  - Come misura di sicurezza aggiuntiva iOS supporta la **cancellazione totale dei dati utente** dopo 10 tentativi di immissione del codice di sblocco.

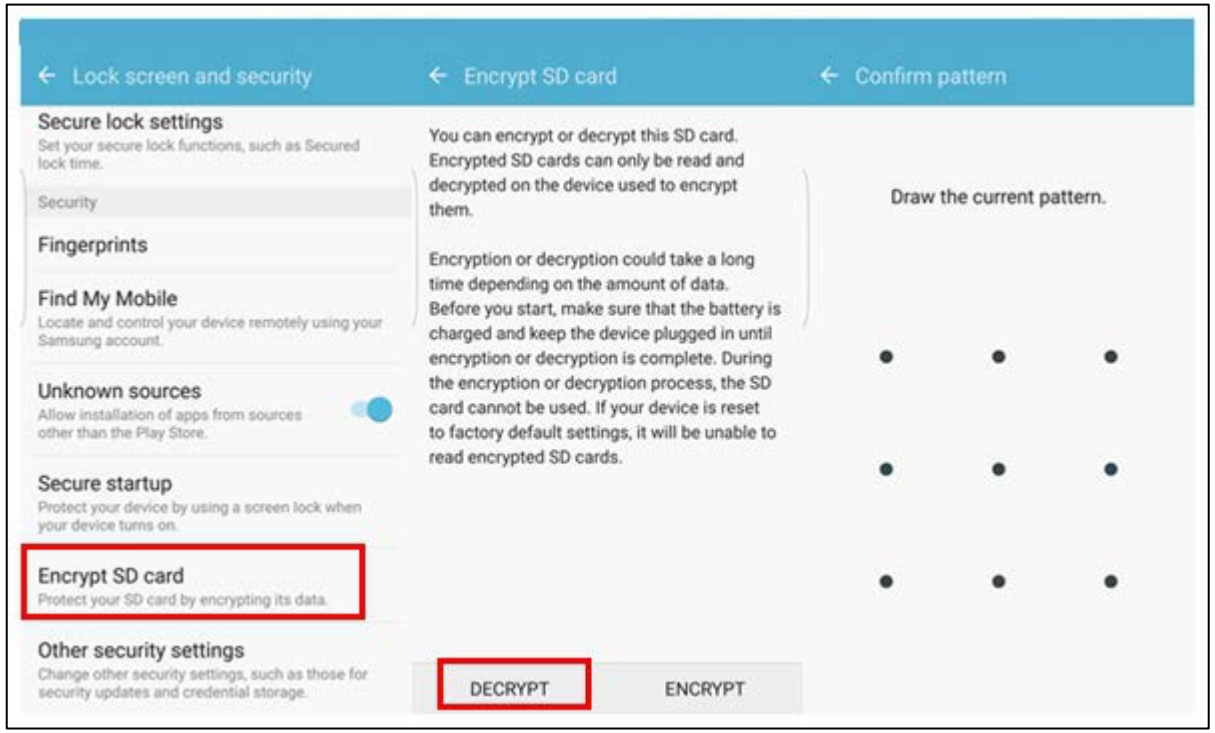
- **Impostazioni → *Touch ID/FaceID e Codice***
- **Inserire il codice di sblocco dell'iPhone**
- **Scorrere l'elenco fino in fondo**
- **Attivare la voce *Inizializza Dati***

7.2 Mobile Security
Cifratura dei dati
Android

- **Cifratura dei dati**
- **Android**
  - Due metodi di cifratura:
    - FDE (Full-disk Encryption - Android 4.4-9)
    - FBE (File-based Encryption - Android 7+, obbligatoria per i dispositivi 10+)
- Per controllare o abilitare la cifratura:
  - ***Impostazioni→Sicurezza→Esegui crittografia telefono***
- Possibilità di cifrare anche la **scheda SD**
  - ***Impostazioni→Sicurezza→Encrypt SD card → Attiva.***
- **Molto importante perché dalle schede SD e MicroSD è possibile recuperare i darti cancellati**

7.2 Mobile Security
Cifratura dei dati
Android

- **Cifratura dei dati**
- **Android**



- Una volta attivata la cifratura della scheda MicroSD, i dati in essa contenuti sono leggibili solo dal dispositivo associato e sbloccato.

7.3 Mobile Security Backup Locale vs Backup Cloud

- **Backup Locale vs Backup Cloud**
- **Backup Locale**
  - **Backup del dispositivo**
    - **PC**
    - **Hard-disk**
  - **Backup di singole applicazioni**
    - **Smartphone**
    - **SD Card**
    - **PC**
    - **Hard-disk**

7.3 Mobile Security Backup Locale vs Backup Cloud

- **Backup Locale vs Backup Cloud**
- **Backup Cloud**
- **Intero dispositivo o singole applicazioni**
- **iCloud (Apple), Google Drive (Android)**

- *WhatsApp* supporta il backup su *Google Drive* e *iCloud*

7.4 Mobile Security
Cifratura del backup

- **Cifratura del backup**
- **Apple**
- Evita l'accesso alla copia di tutti i vostri dati da parte di malintenzionati
- Su iCloud i dati hanno cifratura minima AES 128 bit
- Possibilità di cifratura di backup locali tramite iTunes

7.4 Mobile Security
Cifratura del backup

- **Cifratura del backup**
- **Android**

- Backup cifrato su **Google Drive** usando il codice di sblocco dell'utente

- Backup in locale cifrato a seconda dei dispositivi e dei programmi associati (**Smart Switch** per **Samsung**, **Huawei HiSuite, XiaoMI**…)

7.5 Mobile Security
Jailbreak e root

Jailbreak e root

- Procedure con cui si acquisiscono i massimi privilegi su dispositivi mobili **Apple** (**Jailbreak**) e **Android** (**root**)
- Consentono di accedere a **tutti i dati conservati nei dispositivi**
- Permettono di acquisire anche i **servizi cloud connessi** (Gmail, Dropbox, Facebook, WhatsApp, Instagram etc.)
- **Difficile da fare da remoto**
- **Difficile da fare su dispositivi di fascia alta**
- **Effettuare gli aggiornamenti di sicurezza e utilizzare dispositivi sempre più recenti dei dispositivi è la miglior contromisura**

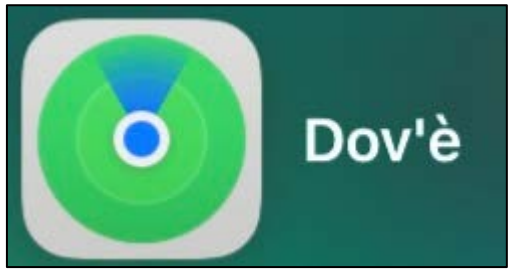
7.6 Mobile Security Geolocalizzazione

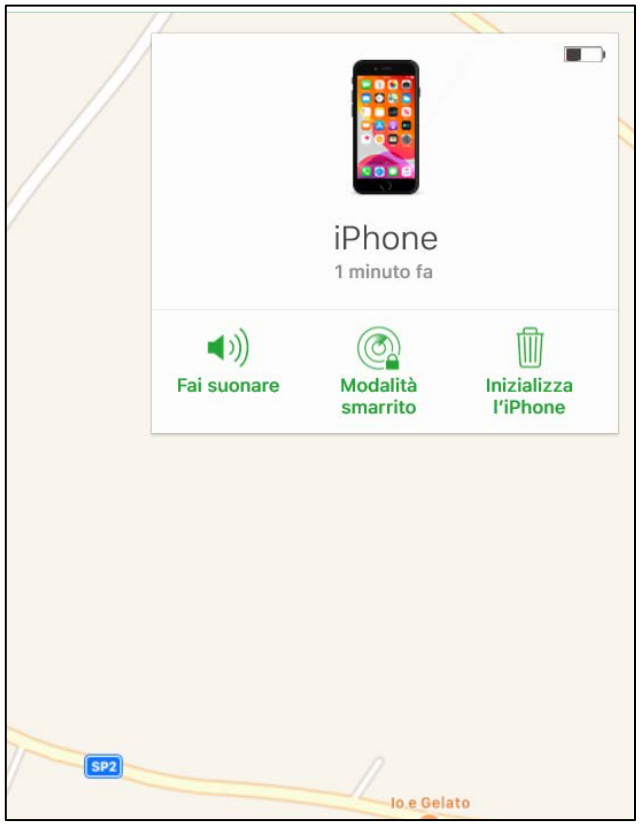
- **Geolocalizzazione**
- Individuazione geografica del luogo in cui si trova un oggetto attraverso apparecchiature in grado di trasmettere segnali a un satellite

- Varie tecniche:
  - **GPS** è basato sui segnali radio ottenuto da satelliti artificiali in orbita attorno alla Terra
  - **Celle della rete telefonica cellulare**
  - **WiFi** o **WLAN**: è basato sul segnale delle diverse fonti WiFi
  - **Rete Internet**: tramite l'**indirizzo IP**

7.6.1 Mobile Security
Geolocalizzazione Apple
Find my iPhone

- **Apple**
  - www.icloud.com/find
  - ***Find my iPhone*** **-** App preinstallata (in italiano «***Dov'è***»)





7.6.1 Mobile Security Geolocalizzazione Apple *Find my iPhone*

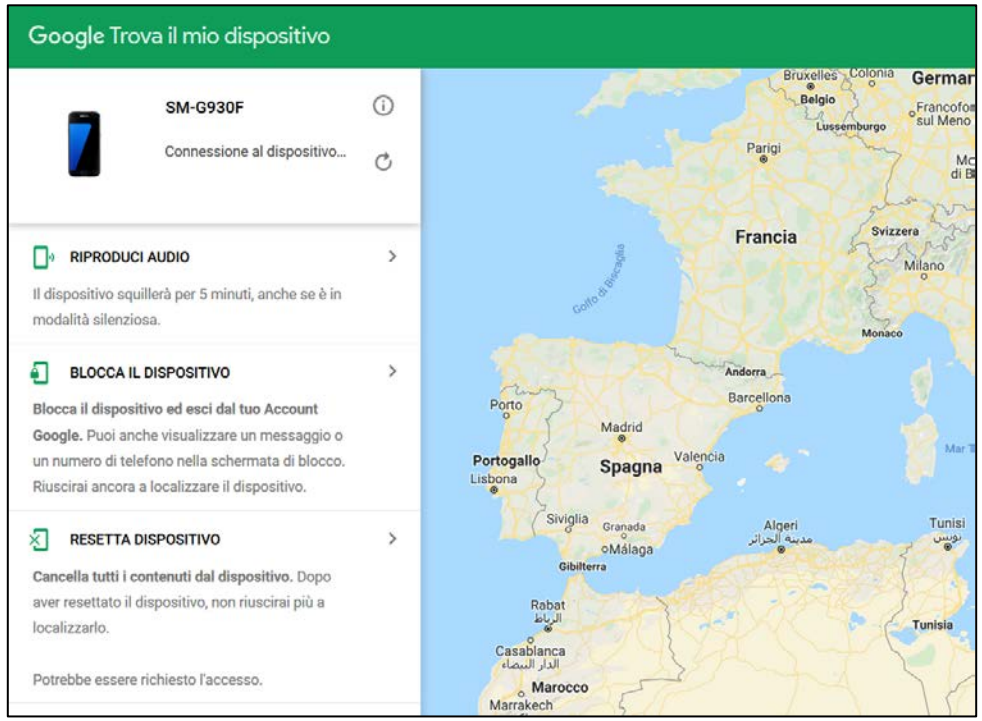
- **Apple**
- Su **iPhone** o **iPad**:

Impostazioni → [nome] → Dov'è →Trova il mio iPhone

7.6.2 Mobile Security
Geolocalizzazione Android
Find my Phone

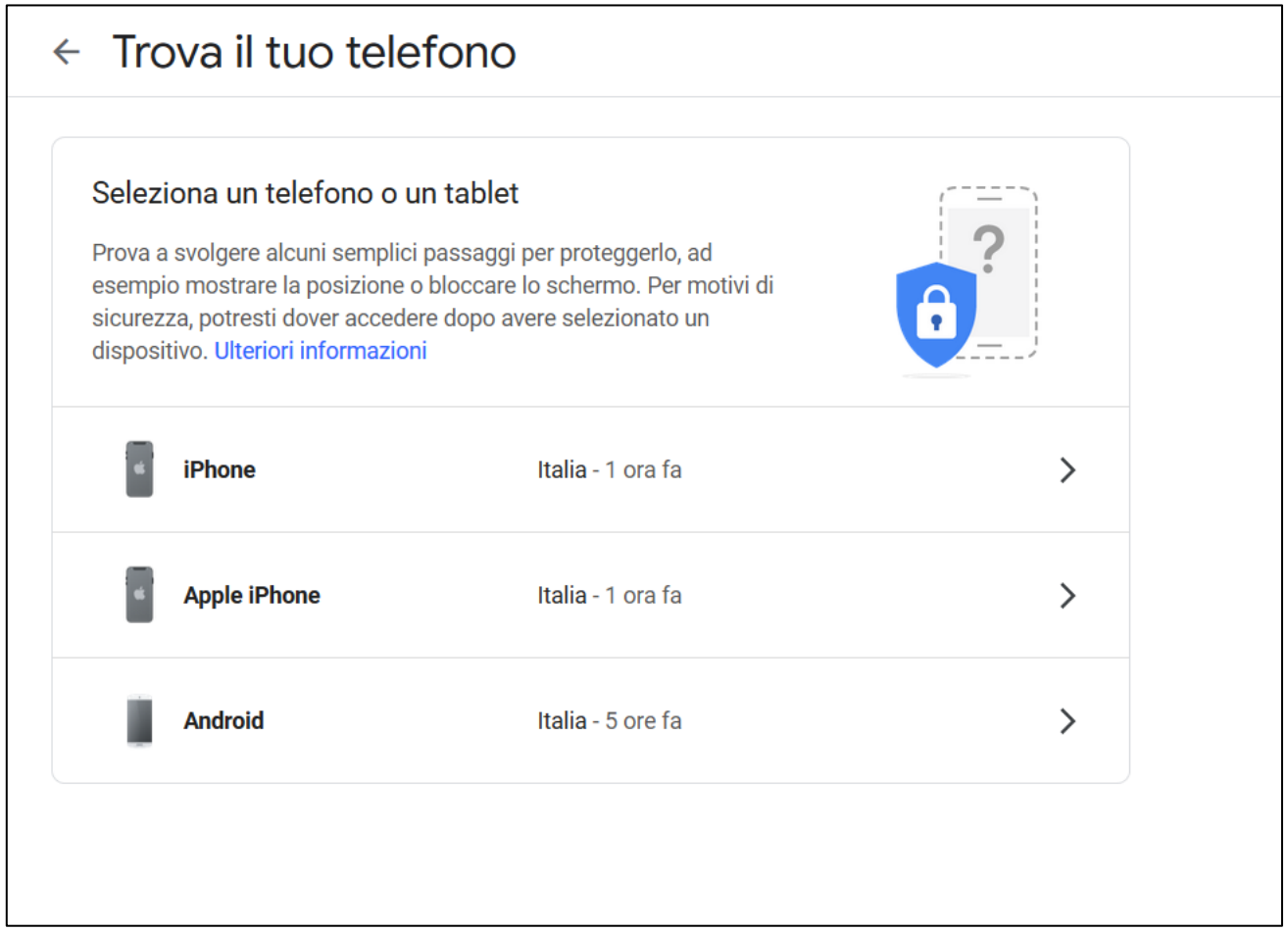
- **Android**
- **android.com/find**
- App «**Trova il mio dispositivo**»

- Necessario **account Google** associato
- Attivare le opzioni di **sicurezza** «**Trova il mio dispositivo**» e «**Posizione**»



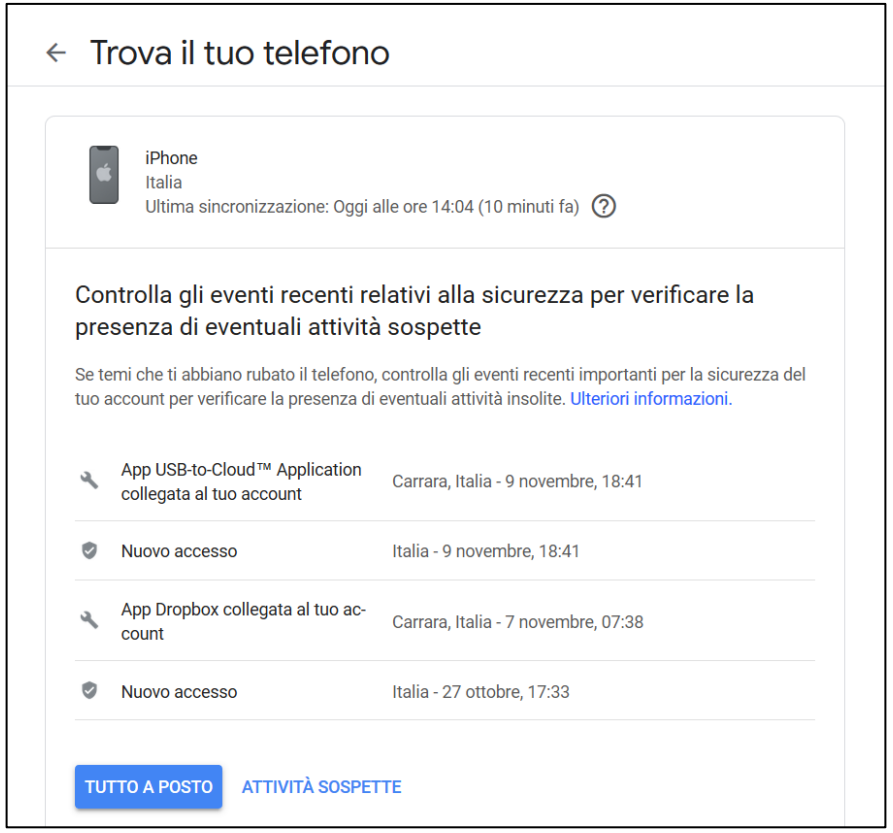
7.6.2 Mobile Security
Geolocalizzazione Google
Find my Phone

- **Google**
- **Find Your Phone**
- **https://myaccount.google.com/find-your-phone**



7.6.2 Mobile Security
Geolocalizzazione Google

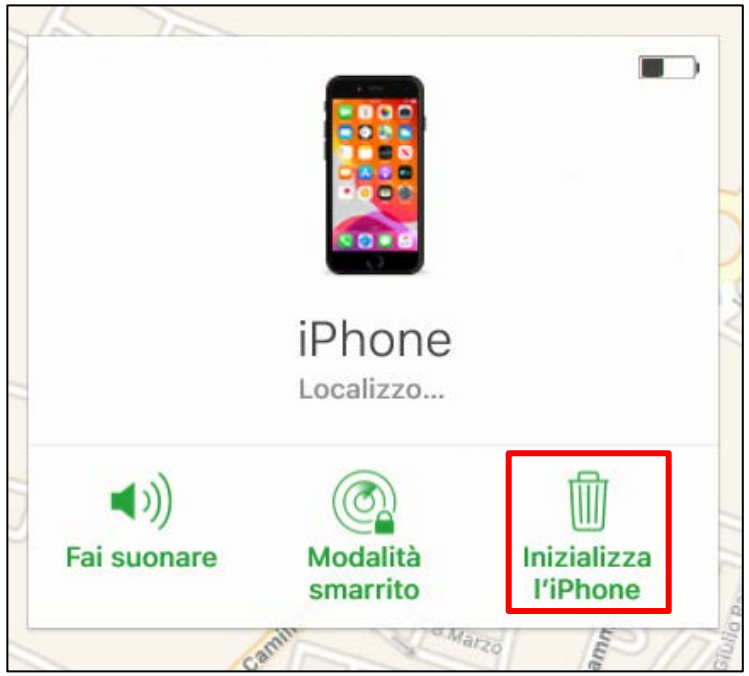
- **Google**
- **Find Your Phone**
- **https://myaccount.google.com/find-your-phone**
- Consente di dissociare l'account **Google** collegato



7.8 Wipe da remoto
iOS

- **Wipe da remoto**
- Opzione «estrema» di sicurezza.
- Riporta il dispositivo alle impostazioni di fabbrica
- **Cancella tutti i dati personali memorizzati**

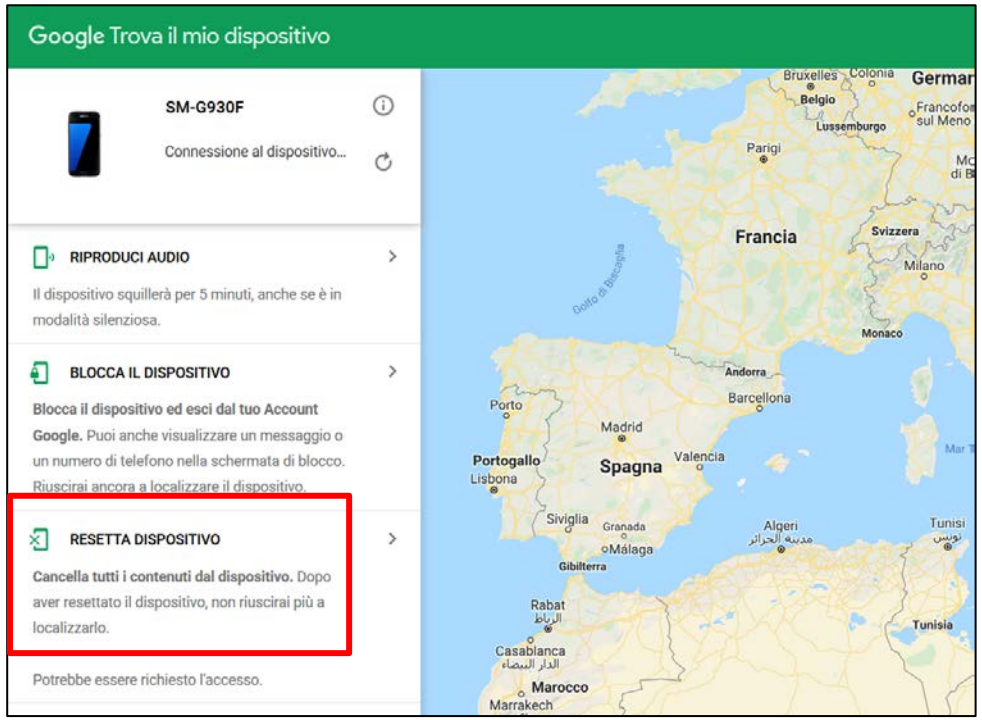
iOS



7.8 Wipe da remoto

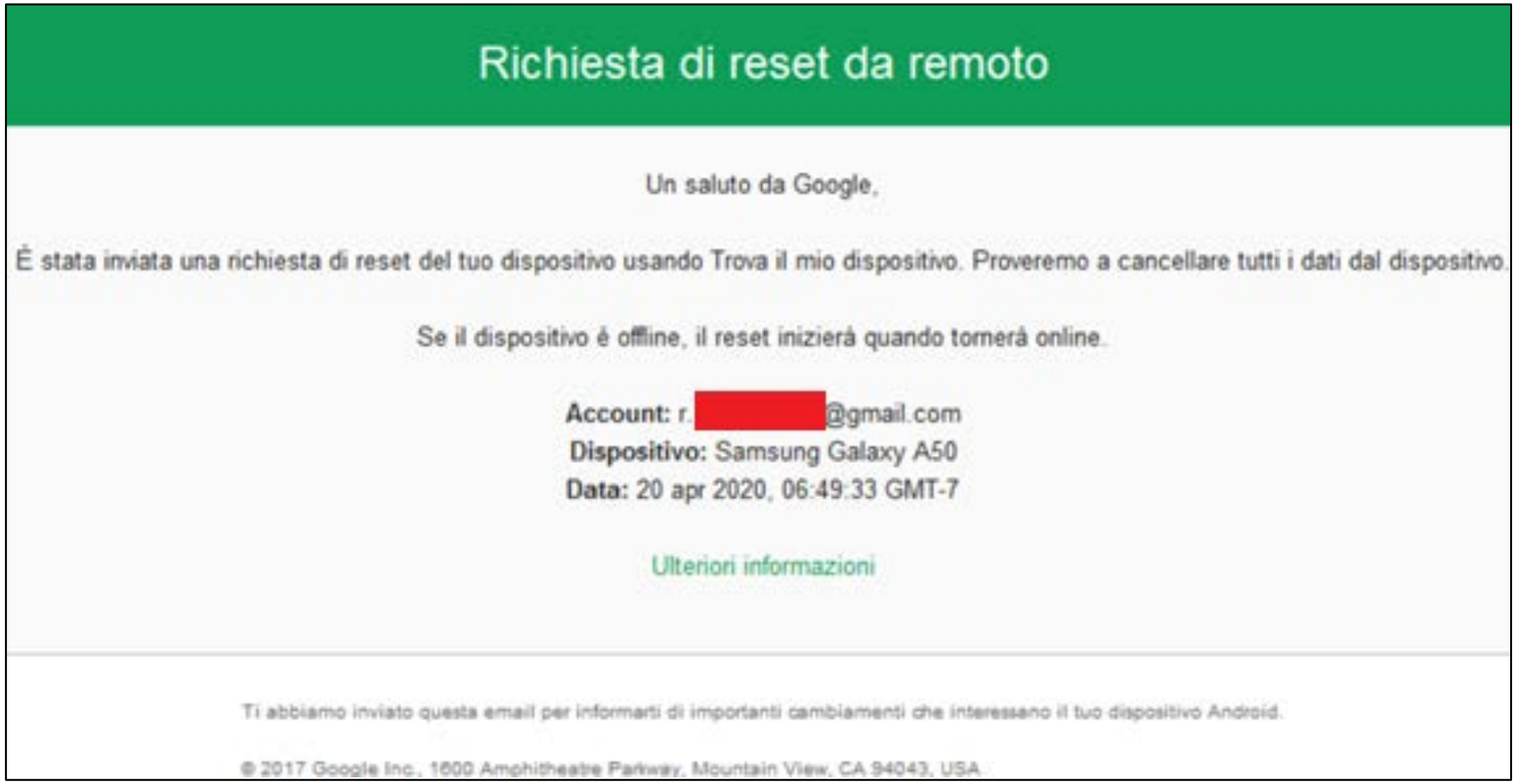
Android

Android



Android

7.8 Wipe da remoto
Android



Richiesta di reset da remoto

Un saluto da Google,

È stata inviata una richiesta di reset del tuo dispositivo usando Trova il mio dispositivo. Proveremo a cancellare tutti i dati dal dispositivo.

Se il dispositivo è offline, il reset inizierà quando tornerà online.

Account: r.[redacted]@gmail.com
Dispositivo: Samsung Galaxy A50
Data: 20 apr 2020, 06:49:33 GMT-7

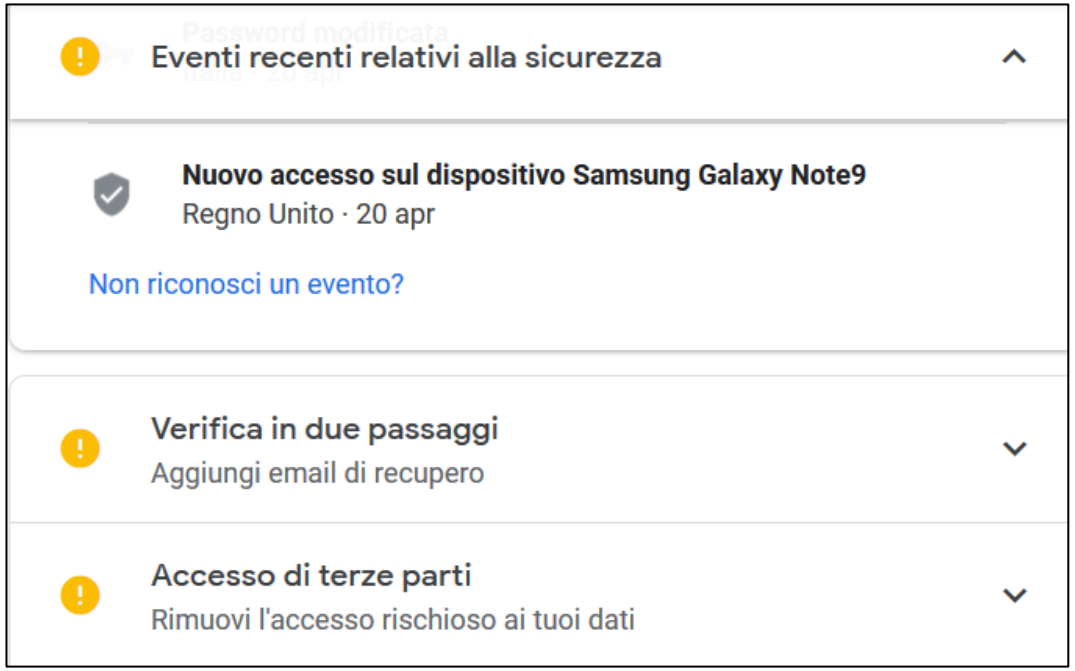
Ulteriori informazioni

Ti abbiamo inviato questa email per informarti di importanti cambiamenti che interessano il tuo dispositivo Android.

© 2017 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Android

7.8 Wipe da remoto
Android



Dalla sezione *Controllo Sicurezza* dell'account Google associato al dispositivo si rileva una geolocalizzazione riferita al Regno Unito, presumibilmente associabile all'utilizzo di un dispositivo di anonimizzazione dell'indirizzo IP, verosimilmente un servizio VPN.

Virtual Private Nework (VPN): software che garantisce privacy, anonimato e sicurezza attraverso un canale di comunicazione logicamente riservato (tunnel **VPN**) e creato sopra un'infrastruttura di rete pubblica. L'utilizzo della VPN consente di mascherare l'indirizzo IP del dispositivo utilizzato, reindirizzandolo sui server che ospitano il servizio e facendo apparire il dispositivo come geolocalizzato in uno stato diverso da quello dell'effettiva provenienza.

7.9 App e sicurezza

- **App e sicurezza**
- Attenzione a cosa installate
- Usare sempre **App Store** e **Google Play per scaricare le app da installare**

Decine di app insicure sull'App Store per iPhone e iPad

Naviga SWZ: Home Page » News

News del 02 Luglio 17 Autore: Stefano Fossati

Decine di **app per iPhone e iPad** mettono tuttora a **rischio i dati sensibili dei loro utenti** comprese le credenziali di accesso ai rispettivi servizi, a causa di una **vulnerabilità** resa nota all'inizio dell'anno e che, in molti casi, **non è mai stata risolta** nonostante siano ormai trascorsi diversi mesi dalla scoperta.

Era stato **Will Strafach**, amministratore delegato di **Sudo Security Group**, a rivelare lo scorso febbraio una lista di **33 popolari app per iOS esposte al rischio di attacch "man-in-the-middle"**, che consentono a ipotetici hacker di **intercettare dati** ne momento in cui vengono trasmessi da un dispositivo a un server remoto. Queste app identificate da Strafach dopo avere verificato migliaia di applicazioni disponibil nell'App Store, a causa di un'errata implementazione del codice stabiliscono una connessione criptata accettando qualsiasi certificato, senza eseguirne correttamente la validazione. Così un eventuale hacker, presente nei paraggi del dispositivo e **connessa alla stessa rete wi-fi**, potrebbe indurre l'app ad **accettare un certificato falso** ed essere così in grado di impossessarsi di **username e password dell'utente**, senza che quest'ultimo peraltro possa accorgersi di nulla.

Simone Moro – macroarea "**Cyber security**"
Università Cagliari – Ingegneria. Laurea in "Ingegneria delle comunicazioni"
Tesi: "**Attacchi avanzati su piattaforma Android: studio, sviluppo e implementazione di software deliberatamente vulnerabile**"
Vincitore nel 2015 «Una Tesi per la Sicurezza Nazionale» del DIS
https://www.patextra.it/AttacchiAvanzatisuPiattaformaAndroid.pdf

7.10 Spyware

Spyware: malware appositamente sviluppato per raccogliere informazioni sull'attività online di un utente senza il suo consenso.

App alla portata di chiunque ed a prezzi accessibili, con le quali è possibile spiare lo smartphone di un’altra persona.

Vengono vendute con lo scopo dichiarato di “controllare lo smartphone dei propri figli”.

Si tratta di programmi la cui installazione nel dispositivo di un terzo (senza la sua autorizzazione) rappresenta un vero e proprio reato.

7.10 Spyware

Articolo 617 bis Codice Penale
Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche

- Chiunque, fuori dei casi consentiti dalla legge [c.p.p. 266-271], al fine di prendere cognizione di una comunicazione o di una conversazione telefonica o telegrafica tra altre persone o comunque a lui non diretta, ovvero di impedirla o di interromperla, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, **mette in altro modo a disposizione di altri o installa apparati**, strumenti, parti di apparati o di strumenti idonei **intercettare**, impedire od interrompere comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni.

- La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.

7.10 Spyware

App tra le più note:

- *Cerberus*
- *FlexiSPY*
- *Hoverwatch*
- *Mobistealth*
- *mSpy*
- *SpyFone*
- *TeenSafe*

Quasi tutte richiedono l'**accesso diretto al dispositivo da spiare da parte dell'attaccante**, per poter essere **installate**.

Importanza di mettere in **sicurezza fisica** e proteggere con **codice di sblocco** i propri dispositivi.

Alcune app si focalizzano solo su alcune applicazioni o funzioni del dispositivo (mail, WhatsApp, chiamate telefoniche etc.)

La maggior parte è in grado di intercettare la maggior parte dell'attività dell'utente fa con il proprio smartphone e di **geolocalizzarlo**.

7.10 Spyware

Installazione da remoto

Meno frequente

Due possibilità:

1. si utilizzano tecniche di **phishing** e **social engineering**, inviando un link attraverso il quale – se cliccato – si

installerà lo spyware.

2. Spwyare nascosti all'interno di applicazioni o giochi gratuiti.

Cosa si può fare:

- Attenzione ai messaggi ricevuti (presenza di link)
- Evitare di installare app di incerta provenienza
- Massima attenzione soprattuto da store di terze parti (Aptoide, F-Droid, Mobogenie, AppMarket etc.)
- Attenzione comunque a eventuali falle di Google Play Store e Apple AppStore

7.10 Spyware

Una volta installato l'attaccante avrà a disposizione un'app o un account web attraverso il quale potrà vedere i dati contenuti nello smartphone della vittima: telefonate, messaggi, e-mail, foto.

Potrà inoltre attivare all'insaputa dell'utente **fotocamera** e **microfono**.

GRAZIE PER L'ATTENZIONE