CYBER SECURITY

La Difesa

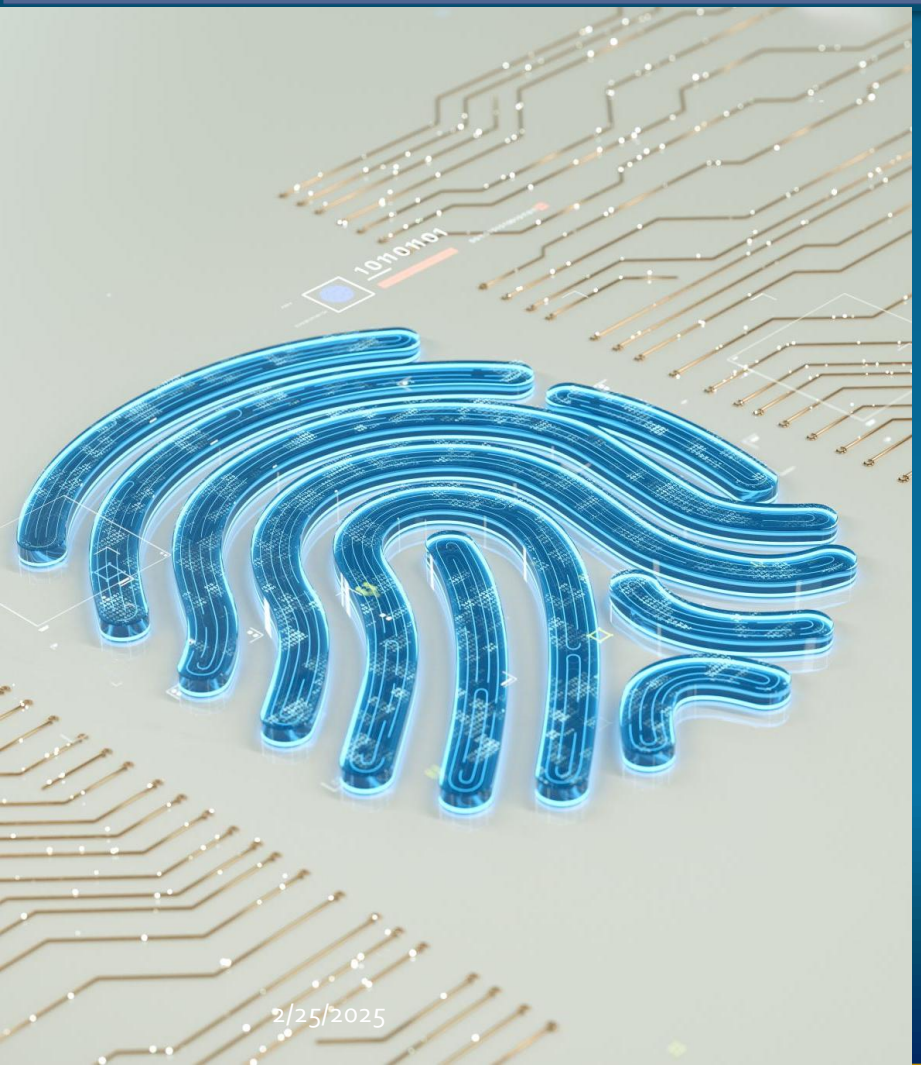
LA DIFESA... AUTEAUTO

AUTENTICAZIONE
&
AUTORIZZAZIONE

La sicurezza FISICA

- Valutazione dei rischi
- Controllo degli accessi
- Sorveglianza video
- Illuminazione adeguata
- Sicurezza dei perimetri
- Sicurezza delle chiavi

LA SICUREZZA FISICA



- Autenticazione Multifattoriale (MFA
- Crittografia dei dati
- Gestione delle Password
- Software di Sicurezza
- Politiche di Accesso
- Monitoraggio e Log degli Accessi
- Aggiornamenti Software
- **Educazione e Formazione**

LA SICUREZZA FISICA

- Disabilitazione delle Porte USB e dei Lettori DVD
- Blocco Fisico delle Porte
- Software di Controllo delle Porte
- Rilevamento di Keylogger
- Crittografia di Dispositivi Esterni
- Politiche di Uso dei Dispositivi
- Monitoraggio Fisico
- **Educazione e Formazione degli Utenti**

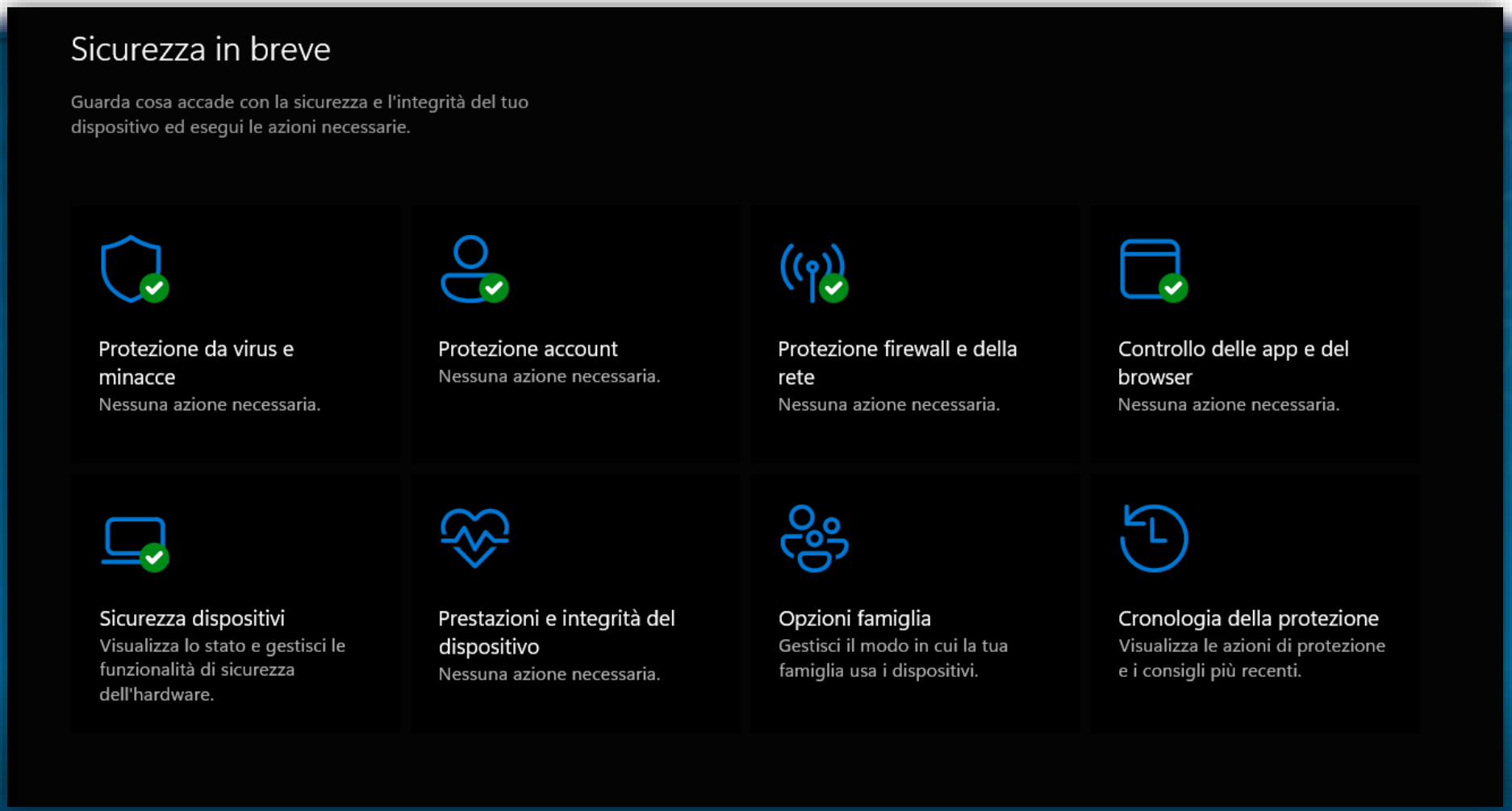
La DIFESA…

- Non abbandonate mai un dispositivo accessibile senza *lock-screen*
  - Pericoli: attacchi fisici e locali
- Impostate delle password decenti
  - Anche nei telefonini http://en.wikipedia.org/wiki/Smudge_attack
  - Sulle impronte digitali vedere:
    - http://punto-informatico.it/4208962/PI/News/ccc-nuovo-contro-impronte-digitali.aspx
    - http://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/
- Dove possibile, cifrate l'intero dispositivo

La difesa: Servizi

- Disabilitare il DHCP libero, impostando i dispositivi autorizzati via mac-address
- Creare zone demilitarizzate
- Creare una sottorete per gli ospiti protetta da password
- Wi-Fi: nascondere SSID
- Rimuovere gli accessi per Everyone
- Gestire capillarmente gli utenti, rimuovendo chi non è più autorizzato

Sicurezza dell'OS



Il software Originale

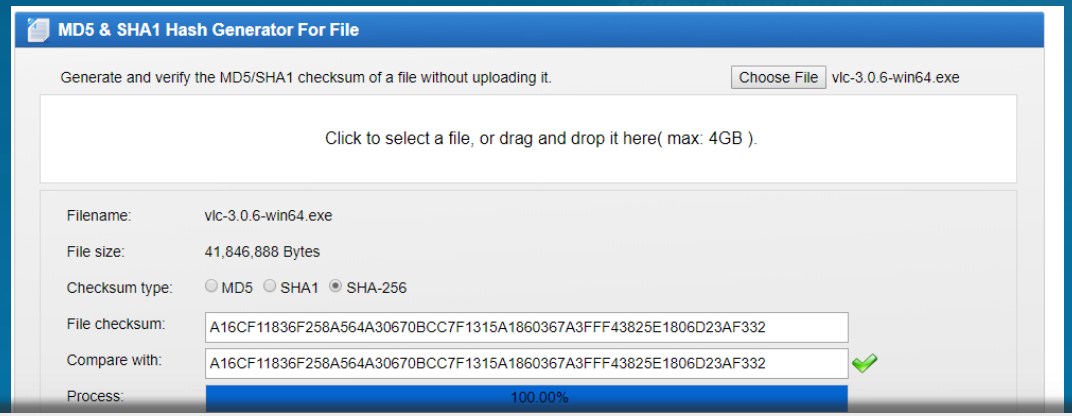
https://get.videolan.org/vlc/3.0.6/win32/vlc-3.0.6-win32.7z

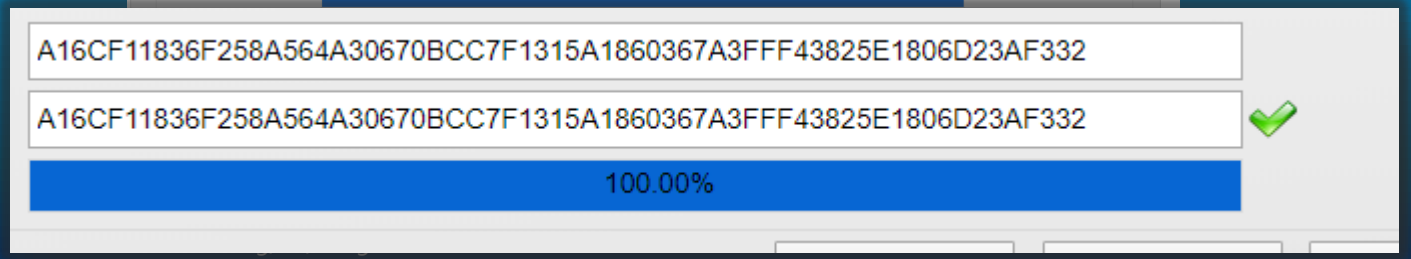
SHA-256 **checksum**:

21ab9733b7bdbf9f5cac031c06cee443fa4873ccb2fff66a966a0beec4fe6cc4

http://www.winmd5.com/

http://onlinemd5.com/





Windows File Hash (powershell)

se non specificato, usa sha256

Get-Filehash ./hashthis.jpg -algorithm md5

Linux File hash (bash)

sha256sum <file>

sha1sum <file>

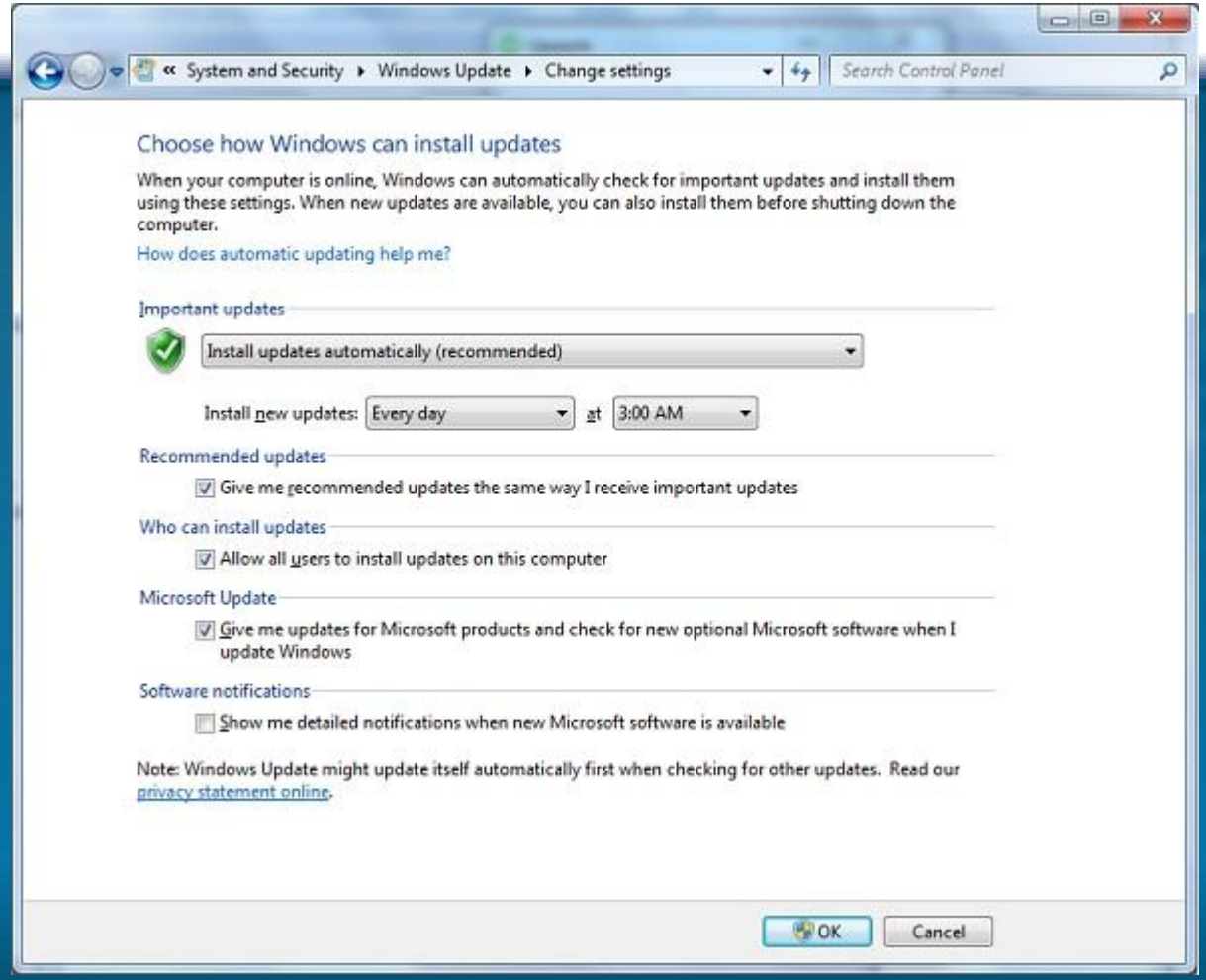
md5sum <file>

La DIFESA... Software

- Tenere aggiornato *tutto* il software
  - sistema operativo
  - antivirus
  - tutte applicazioni (rimuovere quelle non usate)
- Firmware dei vari dispositivi (router, switch, TV, . . .)
- Abilitate gli aggiornamenti automatici, dove possibile
- Nel 2014: "44% of breaches . . . known vulnerabilities, 2–4 years old"
  - www.welivesecurity.com/2015/02/25/top-10-breaches-2014-attacked-old-vulnerabilities-says-hp/
- Evitate:
  - programmi/app di dubbia provenienza (crack, keygen, etc)
  - marketplace non ufficiali (Android/iOS)
  - l'esecuzione automatica di programmi da DVD/USB/. . .

La difesa: HW e Sw

- Parola d'ordine: AGGIORNARE !



Aggiornamenti

- Windows
- Antivirus
- SW di terze parti (p.es. Adobe Acrobat Reader)

- Exploit DB ➔ Vulnerabilità rilevate (exploit-db)

Update: Si tratta di una modifica minore o di una correzione del software o dell'hardware esistente.
Upgrade: Rappresenta un cambiamento maggiore e più significativo rispetto agli update.

La DIFESA... Antivirus

- (Installate e) tenete aggiornato un antivirus
  - (per scegliere può essere utile: https://www.av-test.org/en/antivirus/)
- In caso di file sospetto fatelo esaminare a http://www.virustotal.com/
- Esecuzione in ambienti virtualizzati
  - (per esempio, usando Virtual Box https://www.virtualbox.org/)
- Se il PC rischia di essere infetto:
  - Kaspersky Rescue Disk http://support.kaspersky.com/8093
- Una distribuzione *live* di Linux e F-PROT
  - http://www.f-prot.com/products/home_use/linux/
- ***INUTILE*** usare qualcosa sul sistema operativo infettato

GLI ANTIVIRUS

- Programma in grado di riconoscere e neutralizzare un virus
- Operazioni:
  - Prevenzione
  - Aggiornamento
  - Cura
- CONTROLLI PERIODICI
  - Dischi, RAM e Supporti
- CONTROLLI APERIODICI / CONTINUATIVI
  - Posta elettronica, navigazione e scaricamento WEB
- NO Programmi Sconosciuti NO Macro

SW DI TERZE PARTI

- AV free o pagamento?
  - Search Engine per cercare l'AV che ci va bene
- Prova AVG free
  - Configurazione, Aggiornamento, Scansione, Rimozione minacce, Storico
- Prova Malwarebytes
- Prova AdBlock ➔ Navigazione WEB senza pubblicita'

LA DIFESA... IL WEB

- Cercare di usare sempre HTTPS (controllate la barra degli indirizzi, mettetelo di default ovunque possibile)
  - Flash `e probabilmente la cosa peggiore, disabilitatelo di default: ennesima-falla-in-flash
- Alcuni add-on per i browser:
  - NoScript, disabilita selettivamente JS, Java e Flash https://noscript.net/
  - HTTPS Everywhere https://www.eff.org/https-everywhere
  - AdBlock+, evita di scaricare pubblicità e contenuti potenzialmente dannosi https://adblockplus.org/
  - Disconnect, evita (selettivamente) di essere tracciati https://disconnect.me/
- Infine, non fidatevi ciecamente solo perché ci sono dei lucchetti nella pagina! http://www.troyhunt.com/2011/07/padlock-icon-must-die.html

Sicurezza di rete

- I nostri dispositivi
- Le Reti
- Connessioni di rete
- Sicurezza delle connessioni wireless
- Controllo degli accessi

Gestione sicura dei Dati

- **Protezione e Backup**

  processo atto a ottenere una o più copie di riserva dei dati, da utilizzare in caso di eventi malevoli accidentali

- **Privacy**

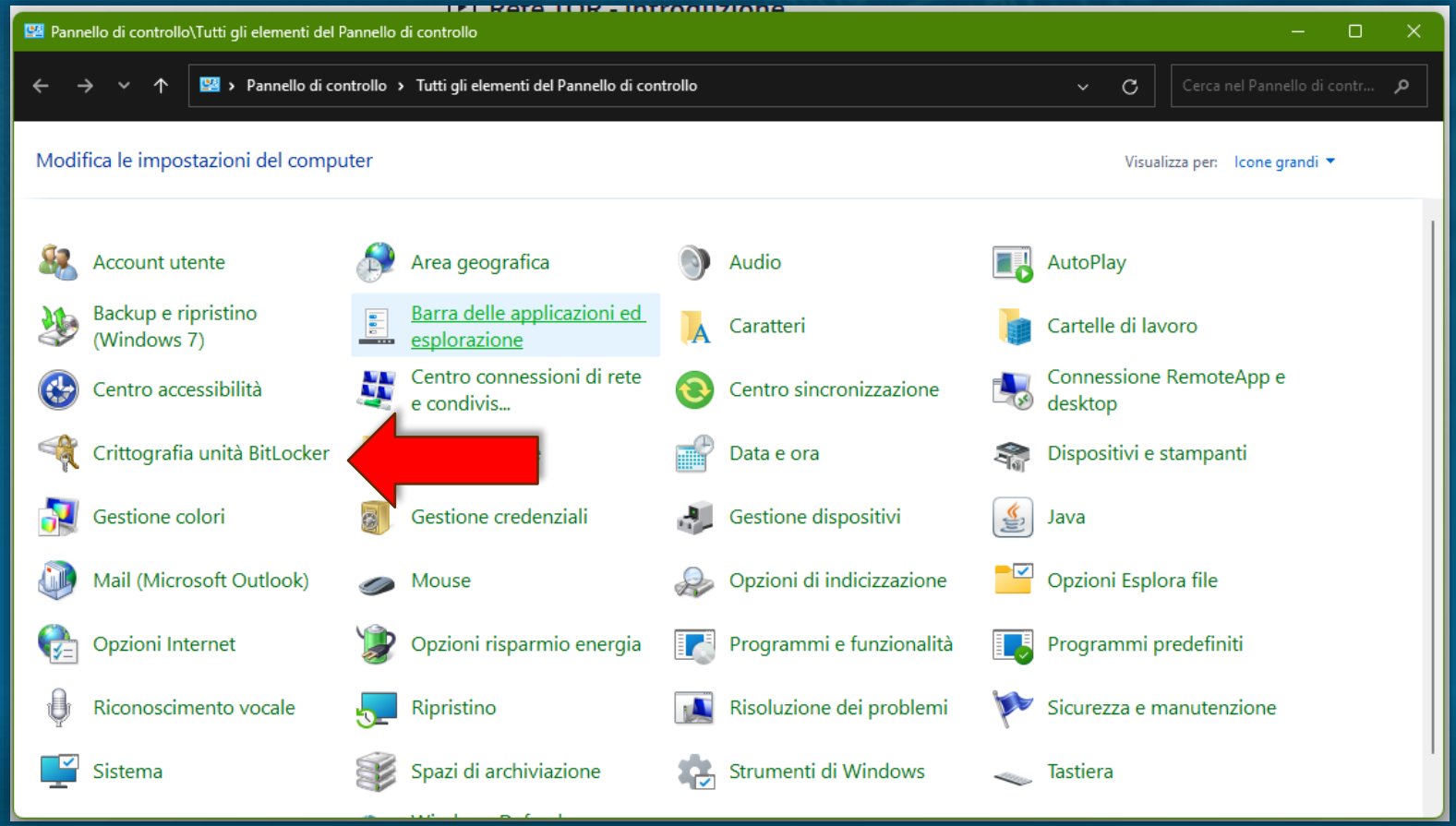
- **Crittografia**

Backup

- **Locale** VS **Cloud**
- MS OneDrive ➔ Test in line / off line
  - Free ➔ 5GB
  - Configurazione cartelle, file, comportamenti
  - Accesso locale / web

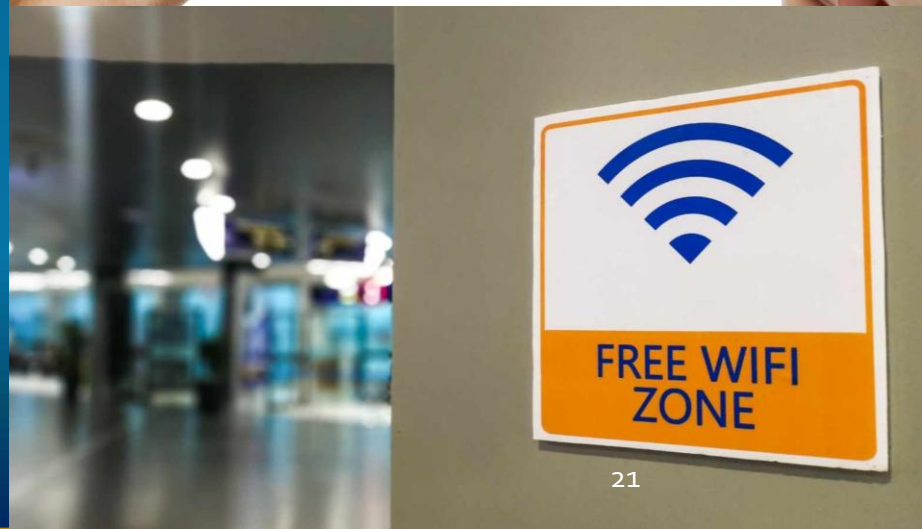
Cifratura del disco

- **BitLocker** (*video*)
- **Veracrypt** (*link* - *video*)



La DIFESA... il WiFi

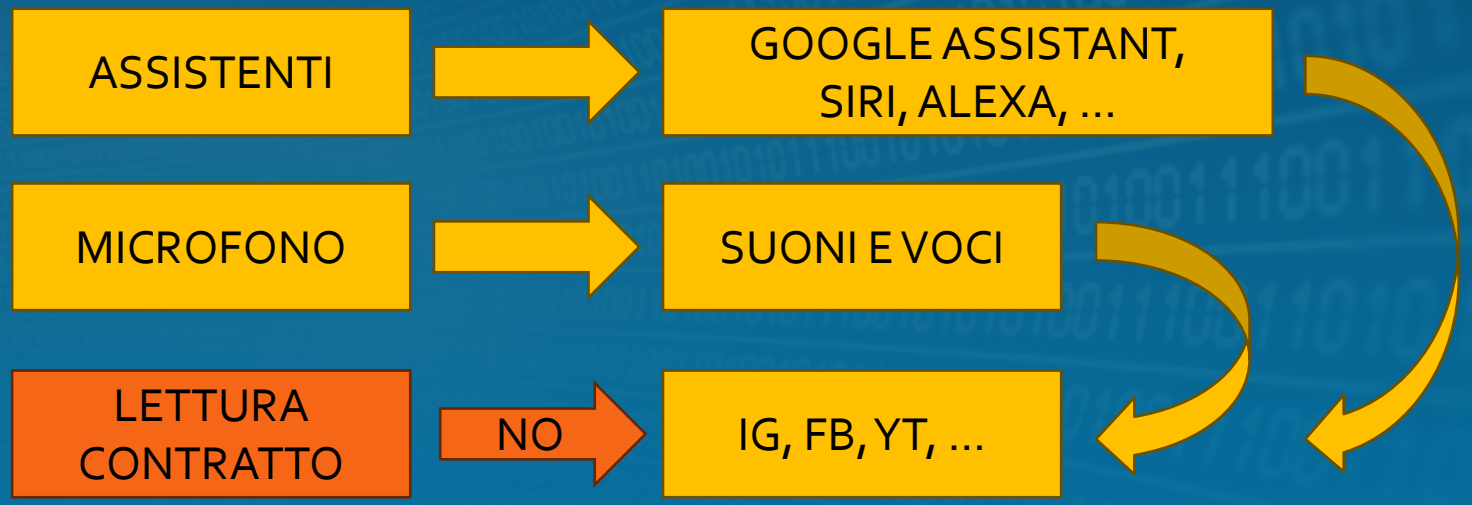
- I WiFi pubblici
  - Attacchi Man-in-the-Middle (MITM)
  - Spoofing
  - Sniffing e Snooping (spionaggio)
  - Malware
  - Assenza di crittografia
- Il QRCode
  - QR Code Malevoli
  - Phishing



Reti WiFi Pubbliche

- articolo europol
- Black Hat ➔ hotspot stesso nome (simile) al wi-fi vero
- Main in the Middle
- Sniffing di pacchetti

LO SMARTPHONE CI SPIA: EVITIAMOLO…



DISATTIVARE IL MICROFONO
REVOCARE AUTORIZZAZIONI ALLE APP

La vera "scatola nera" dell'auto? È dentro lo smartphone

- Ife360
- MyRadar
- GasBuddy
- …

- Comportamento alla guida

Feedback
- Sicurezza
- Consumi

- BROKER Assicurazioni

RIAVVIARE LO SMARTPHONE UNA VOLTA A SETTIMANA È UTILE CONTRO GLI HACKER?

SI, MA SOLO SE

L'eventuale malware **non ha caratteristiche di persistenza** in memoria *(praticamente tutti ce l'hanno)*

QUINDI NO ! PRATICAMENTE NON SERVE !

PROTEGGERE LO SMARTPHONE SI PUÒ?

REGOLE BASE

- Non utilizzare reti Wi-Fi pubbliche
- Non ricaricare smartphone (ma anche tablet e laptop) usando stazioni di ricarica pubbliche (stazioni, centri commerciali e così via)
- Non aprire allegati e link condivisi da contatti sospetti
- Scaricare aggiornamenti software e/o patch di sicurezza il prima possibile
- Disabilitare il Bluetooth quando non in uso
- Disabilitare i servizi di localizzazione quando non sono necessari
- Installare applicazioni solo da fonti attendibili, come Play Store e App Store
- Utilizzare un codice per l'accesso al dispositivo e, sui dispositivi che lo consentono, utilizzare un metodo di autenticazione biometrica, come il Face ID