IT SECURITY

SICUREZZA INFORMATICA

Nuova ECDL – Modulo 5

OBIETTIVI DEL MODULO

- Comprendere l'importanza di rendere sicure informazioni e dati, e identificare i principi per assicurare protezione, conservazione e controllo dei dati e della riservatezza (privacy).
- Riconoscere le minacce alla sicurezza personale, quali il furto di identità, e le potenziali minacce ai dati, derivanti ad esempio dal cloud computing.
- Saper usare password e cifratura per mettere in sicurezza i file e i dati.
- Comprendere le minacce associate al malware, essere in grado di proteggere un computer, un dispositivo mobile o una rete dal malware e far fronte agli attacchi del malware.

OBIETTIVI DEL MODULO

- Riconoscere i comuni tipi di sicurezza associati alle reti cablate e wireless, ed essere in grado di usare firewall e hotspot personali.
- Proteggere un computer o un dispositivo mobile da accessi non autorizzati ed essere in grado di gestire e aggiornare in sicurezza le password.
- Usare impostazioni adeguate per il browser web, comprendere come verificare l'autenticità dei siti web e navigare nel World Wide Web in modo sicuro.
- Comprendere i problemi di sicurezza associati all'uso della posta elettronica, delle reti sociali, del protocollo VoIP, della messaggistica istantanea e dei dispositivi mobili.
- Eseguire copie di sicurezza e ripristinare i dati sia localmente che da dischi sul cloud, ed eliminare dati e dispositivi in modo sicuro.

CONCETTI BASE

- In questa sezione saranno illustrati i concetti di base della SICUREZZA INFORMATICA presentando le minacce (spesso giunte da internet) per i dati, le informazioni, i file e le persone.
  Le minacce possono venire da fattori :
  - naturali
  - umani
  - dall'uso del Cloud Computing
- Saranno analizzate le misure di prevenzione e gli strumenti di protezione riguardo:
  - sicurezza dati
  - sicurezza persone
  - sicurezza delle informazioni
  - sicurezza file

5.1. CONCETTI DI SICUREZZA

MODULO 5 - UNITÀ 1

5.1.1. DATI E INFORMAZIONI

- **DATO** è ciò che può essere memorizzato in formati diversi (numeri, testi, immagini, suoni); è ciò che deve essere elaborato.
- **INFORMAZIONE** è il risultato della elaborazione dei DATI; da un significato ai dati a seconda del contesto

5.1.2.1. I CRIMINI INFORMATICI

- E' un **crimine informatico** l'attività criminale fatta con l'utilizzo della tecnologia dell'informazione (hardware o software).
- Le ICT possono essere usate illegalmente per:
  - accesso non autorizzato a dati
  - cancellazione o alterazione dei dati
  - intercettazione dei dati in rete
  - diffusione di virus e malware
  - interruzione di servizio (DoS)
  - furto di identità
  - frodi elettroniche

5.1.2.2. HACKING

- **HACKING** = uso della propria creatività per risolvere un problema di questioni complesse al fine di accrescere la conoscenza della collettività.
- "*to hack*" = intaccare cioè «intaccare» un problema un po' alla volta per giungere ad una soluzione.
- Non ha quindi un'accezione negativa, è l'azione di tanti professionisti che mettono alla prova la vulnerabilità di un sistema, per apportare modifiche e miglioramenti. **HACKING ETICO**

5.1.1.3. MINACCE AI DATI DA SINGOLI INDIVIDUI

- La cancellazione accidentale dei dati per sbadataggine spesso dovuta a interfacce che portano a cancellare intere cartelle con un clic.
  - Il cestino non sempre salva temporaneamente
- Smaltimento delle memorie di massa (pen drive e hd) sempre più piccole e maneggevoli.
- Comportamenti dolosi fatti intenzionalmente quando si lascia il Pc accesso o aperto il proprio account senza logout.
  - Copiatura/cancellazione dati.
- Danneggiamento dei componenti hardware o inserimento di malware che danneggiano o copiano dati.

5.1.1.4.A. MINACCE PROVOCATE DA EVENTI STRAORDINARI

- Tra le minacce di forza maggiore ve ne sono alcune che possono avere un peso notevole sulla sicurezza dei dati.
- Minacce che dipendono dall'ambiente (inondazioni, terremoti, guerra, terrorismo)
  - In questi casi la perdita dei dati potrebbe essere definitiva
- la Protezione può avvenire:
  - infrastrutture in zone sicure
  - impianti antincendio; impianti elettrici con standard di sicurezza
  - backup dei dati
  - centri di elaborazione dati in zone geografiche distanti (mirroring)

5.1.1.4..B MINACCE PROVOCATE DA EVENTI STRAORDINARI

- Altri possibili interventi:
  - installazioni di gruppi di continuità (UPS) in caso di interruzione dell'energia.
  - Installazione di sistemi per l'accesso controllato alla sala computer;
  - Aggiornamento del personale sulle norme di sicurezza informatica;
  - Per le grandi aziende, banche, per lo Stato è necessario pensare ad un **Disaster Recovery Plan** (Piano di soccorso in caso di disastro) in modo che in caso di necessità si riparta in pochi minuti. Servono a questo i sistemi funzionanti in mirror (in parallelo).

5.1.1.5. MINACCE DALL'USO DEL CLOUD COMPUTING

- L'uso del cloud ha avuto uno sviluppo notevole negli ultimi anni. Grazie alla connessione alla rete Il cloud permette di memorizzare, elaborare, produrre e condividere informazioni.
- Possibili minacce:
  - controllo sui dati.
    - Quanto è memorizzato sul cloud è a disposizione dell'utente, ma anche dell'ente proprietario del servizio. Il malfunzionamento dell'hardware (o della linea internet) potrebbero non permettere l'accesso ai dati
  - la potenziale perdita di riservatezza.
    - La condivisione dei dati è un bene, prestando attenzione a cosa viene condiviso per la perdita della privacy.

5.1.2.1. SICUREZZA DELLE INFORMAZIONI

- Le caratteristiche delle informazioni sicure sono 3:
  - Confidenzialità (la riservatezza)
    - l'accesso alle informazioni riservate solo alle persone previste
  - Integrità
    - necessità di adottare tutte le precauzioni perché le informazioni sia uguali a quelle originali
  - Disponibilità
    - necessità di adottare tutti i provvedimenti perché l'accesso ai dati sia sempre possibile da qualsiasi luogo.

5.1.2.2. PROTEZIONE DELLE INFORMAZIONI PERSONALI

- Le **informazioni personali** sono quelle legate ad una persona fisica e ne determina l'identificazione, indicano le sue convinzioni politiche, religiose, lo stile di vita, salute, relazioni personali o situazione economica.
- la tutela della privacy è regolata da un codice (**Testo Unico sulla privacy**) e supervisionata dal **Garante per la privacy**
- Particolarmente
  - i dati identificativi
  - i dati sensibili
  - i dati giudiziari
- Il furto di informazioni personali può avere gravi conseguenze, per questo vanno protette per evitare frodi.

5.1.2.2. PROTEZIONE INFORMAZIONI DI LAVORO

- L'uso dei dispositivi mobili ha semplificato anche il lavoro (*smart working*), ma ha anche esposto a maggiori rischi dati e informazioni. Le minacce:
  - furto del dispositivo e delle informazioni in esso contenute
  - uso illecito delle informazioni (divulgazione, accesso a codici di autenticazione)
  - perdite accidentali, manomissioni e sabotaggi (cancellazione di date), malware.
- Necessarie delle protezioni sia a livello di hardware (impronte digitali) sia a livello di software (Pin, username, password).
- Non lasciare dispositivi incustoditi.

5.1.2.4. PRINCIPI COMUNI PER LA PROTEZIONE DATI

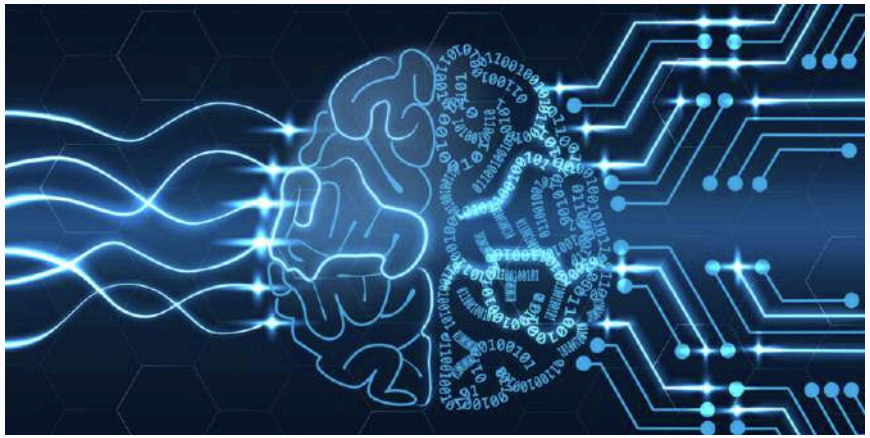
- Nel **Testo Unico sulla privacy** sono riportate le modalità, e i principi per la protezione, conservazione e controllo dei dati e della riservatezza in relazione ai soggetti proprietari dei dati e ai soggetti che li tutelano
- Principi fondamentali:
  - **Trasparenza:** modalità con cui i dati vengono raccolte e protetti deve essere chiara.
  - **Scopi Legittimi:** chi raccoglie i custodisce i dati deve medicare chiaramente gli scopi e la necessità della raccolta stessa dei dati
  - **Proporzionalità delle misure in rapporto ai da**nni: le misure di sicurezza per la protezione dei dati adeguate alle conseguenze che deriverebbero dalla perdita dei dati

5.1.2.5. SOGGETTI E CONTROLLORI DEI DATI

- Nella protezione dei dati ci sono due figure ai quali si applicano i principi di protezione, conservazione, controllo dei dati e della riservatezza:
- **Soggetto dei dati** = chi fornisce i propri dati personali ha il diritto di essere informato come vengono trattati i propri dati e si può opporre che vengano usati per fini pubblicitari o commerciali e alla loro vendita.
- **Controllore dei dati** = chi custodisce i dati e non ne è proprietario. Ha l'obbligo di conservare i dati il tempo necessario per gli scopi per cui sono stati raccolti e proteggere i dati da intrusioni, con controlli per garantire riservatezza, integrità.

5.1.2.6. LINEE GUIDA E POLITICHE PER L'ICT

- E' importante definire le politiche per il loro utilizzo delle tecnologie ICT creando **Linee Guida** che ne regolino l'utilizzo.
- Livelli da tenere presente:
  - **Politica di sicurezza aziendale** = come l'azienda intende proteggere le informazioni
  - **Politica di sicurezza per il sistema informatico**, come deve essere tutelato il sistema informatico.
  - **Politica di sicurezza tecnica**, cosa si vuole proteggere.
- Vengono quindi definite le **Linee Guida** per l'uso delle ICT con le procedure per l'utilizzo corretto secondo le necessità dell'azienda. Esse vengono divulgate dal **Responsabile per le risorse ICT**.



5.1.3.1. INGEGNERIA SOCIALE E SUE IMPLICAZIONI

- Il modo più semplice per agitare la sicurezza dei dati è farsi rivelare i dati e le informazioni da chi le conosce.
- **INGEGNERIA SOCIALE** = osservazione di una persona, spacciandosi per altri, al fine di carpire le conoscenze utili ad agire.
- Di solito segue un procedimento in 3 fasi:
  - raccolta delle informazioni (footprinting);
  - verifica delle informazioni
  - utilizzo delle informazioni

5.1.3.2. METODI DELL'INGEGNERIA SOCIALE

- Tre sono i metodi per rubare le informazioni sono i modo più semplice per agitare la sicurezza dei dati è farsi rivelare i dati e le informazioni da chi le conosce.
- **INGEGNERIA SOCIALE** = osservazione di una persona, spacciandosi per un'altra persona, al fine di carpire le conoscenze utili ad agire.
- **PHISHING** (to fish = pescare a far abboccare) è cercare di carpire informazioni utili attraverso "falsi siti gemelli" o attraverso mail "cloni" di aziende e di banche.
- **SHOULDER SURFING** = sbirciare di nascosto chi digita i codici, mentre inserisce i dati di accesso.

5.1.3.3-4. FURTO DI IDENTITÀ

- Per furto di ritentata è assumere l'identità "digitale" di un altro attraverso i suoi dati personali
  - Può avvenire sul posto di lavoro, nella vita economica, sui social network (diffamazione), (truffe) finanziarie.
  - Per la conoscenza di dati utili si possono utilizzare oggetti comuni: ricevute bancarie, ricevute carta di credito; oggetti lasciati incautamente cestinate (*information diving* o *trashing*);
- **Skimming** (to skim = strisciare, sfiorare) cioè rubare i dati incorporati nei badge a carte di credito passandoli nei dispositivi utilizzati per leggere i dati.
- **Pretexting** (la stangata) ricostruzione di uno scenario pieno di bugie che sembrano reali alla vittima.

5.1.4.1. LE MACRO: EFFETTI ATTIVARE/DISATTIVARE

- **Macro** = Comandi che si attivano automaticamente dall'applicazione all'apertura del file.
- Serve per risparmiare tempo attivando operazioni frequenti.
  - Ma una macro può essere infettata da un virus e quindi può danneggiare il file, l'applicazione che la utilizza all'intero sistema che la ospita.
- In caso di dubbio della provenienza di una macro o del suo contenuto, è bene non attivare le macro o comunque disabilitarle.

5.1.4.2. LA CIFRATURA: VANTAGGI E LIMITI

- La Cifratura o crittografia rende inutilizzabili i dati contenuti all'interno del file qualora la password sia stata acquisita in modo ingannevole.
- Ne garantisce la riservatezza con 2 elementi:
  - l'algoritmo crittografico (pubblico)
    - è un procedimento matematico con cui i dati diventano incomprensibili ed è conosciuta da tutti
  - una chiave segreta
    - è usata per cifrare e decifrare il documento secondo il procedimento stabilito dall'algoritmo
- Il grado di sicurezza di una cifratura dipende dalla bontà dell'algoritmo e della segretezza e lunghezza della chiave in bit
- Il Limite è dato dal fatto che potrebbe non essere disponibile la Chiave quando serve.

5.1.4.3-4 SICUREZZA DEI FILE

- E' possibile rendere visibile il contenuto di un file, di una cartella o di un disco solo a chi è in possesso della "chiave di accesso".
  - impostare una password direttamente dal programma di gestione del file (word, excel,…) o dal sistema operativo che gestisce la cartella o l'hard disk:
    - file → Informazioni → Autorizzazione → ok
  - Per una cartella si può impostare la password direttamente sul programma di compressione (WinRar o 7zip)

5.2. MALWARE

MODULO 5 - UNITÀ 2

5.2.1.1. MALWARE: TROJAN, BACKDOOR, ROOTKIT

- **Malware** (*Malicious* + *software*) = programma maligno, un software creato per danneggiare un computer, fargli fare operazioni non autorizzate, danneggiando dati e programmi.
  Si auto-installa nel sistema operativo e si nasconde nei programmi nella procedura di **boot** e si esegue ogni volta che si avvia il computer o il programma ospite, Trojan.
  Il **trojan** può attivare una **backdoor** (porta di servizio nascosta) una possibilità di accesso per la gestione del computer da remoto

- Il **rootkit** un programma che permette di assumere il ruolo di amministratore (**root**) da remoto su un computer. In questo modo può modificare o eliminare le misure di sicurezza.

5.2.1.2. COME FUNZIONANO I MALWARE

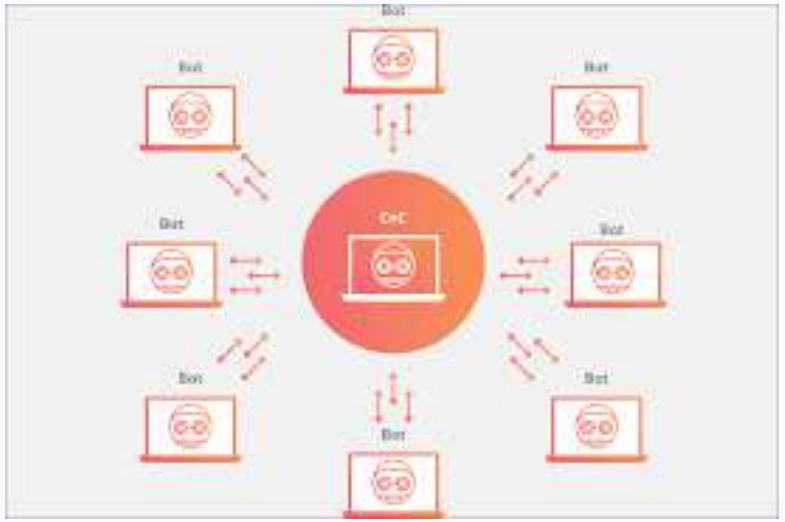
- Alcuni malware sono “infettivi” possono contagiare altri file, replicandosi.
- Il file infetto può essere trasmesso in modo inconsapevole attraverso la posta elettronica.
- Il "programma/virus" copia se stesso in file eseguibili in modo tale che nel momento in cui viene eseguito contagia il computer/sistema.
- Il worm (verme) è un file eseguibile non si deve agganciare a un file eseguibile ma alla posta elettronica, intercetta quindi la rubrica e invia una copia di se stesso in allegato agli indirizzi presenti.

5.2.1.3. TIPI DI MALWARE 1

- Alcuni malware possono avere la funzione di rubare dei dati sensibili, come rubare l'identità dell'utente per truffe o per estorcere qualcosa per evitarne la divulgazione.
  - **keylogger** = il programma registra la digitazione dei tasti e li invia ad un altro computer
  - **Adware** = un software che durante l'esecuzione con insistenza mostra pubblicità del software per migliorarne le prestazioni, o altri software.
    Alcuni si agganciano al browser modificando la ricerca, o perfino lo stesso motore di ricerca, ne registrano la cronologia e la comunicano a server remoti.
  - **Spyware** = un programma che raccoglie informazioni e le invia ad server per inviare pubblicità mirata.

5.2.1.3. TIPI DI MALWARE 2

- Altri tipi di malware:
  - **Botnet** (robot, network) = Insieme di programmi che interagiscono tra di loro e sono collegati a programmi installati sui computer degli utenti costringendoli a fare operazioni specifiche
  - Costituita da 3 elementi fondamentali:
    - i **bot**: infettano i target e li rendono parte della botnet (singoli computer)
    - un **command & control** server (C&C): permette di inviare comandi ai bot e di gestire la **botnet;** (te computer gestori
    - un **botmaster**: persona che gestisce la **botnet** (chi gestisce il tutto)



5.2.1.3. TIPI DI MALWARE 3

- Altri malware ancora:
  - **Ransomware** (software riscatto) software che dal computer su cui si sono installati criptano il contenuto sulle varie memorie di massa rendendoli inutilizzabili. Per avere la "chiave" di decrittazione è necessario pagare un riscatto.
  - **Dialer** = programma che modifica i parametri di connessione del computer a internet, quando per questa operazione è necessario comporre un numero telefonico. Questa modifica porta su una utenza a pagamento lucrando sulla connessione. Il costo non è accreditato al gestore ma alla società titolare della numerazione.

5.2.2.1.A. COME FUNZIONA L'ANTIVIRUS

- Il programma antivirus una volta installato e attivo in background. Controlla la sicurezza dei file, sia in locale che di quelli scaricati come allegati.
- In un database conserva le impronte virali (definizioni) dei malware, l'insieme di comandi che li attivano, vengono raffrontate con i programmi eseguiti dal computer. Inoltre fa in modo che il programma consideri sospetto/blocchi i file che compiono specifiche operazioni.
- Riconosciuto il file viene segnalato in modo da essere ripulito o cestinato.
- Può proporre anche una quarantena, cioè viene messo in una cartella senza essere eseguito, in questo modo si può valutare con calma come agire

5.2.2.1.B. LIMITI DELL'ANTIVIRUS

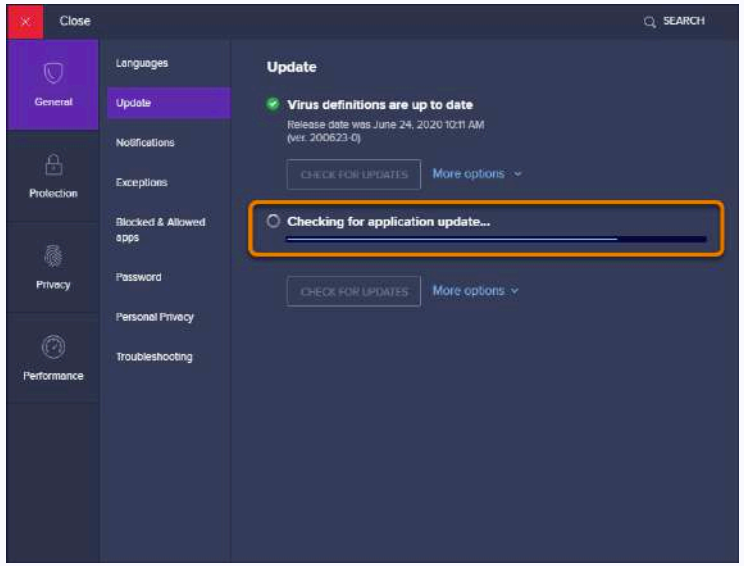
- L'antivirus va lasciato attivo in background in modo che agisca automaticamente, quindi una parte della memoria resta dedicata.
- I file possono essere riconosciuti come sospetti, ma sono leciti (falso positivo), ma comunque ne impedisce l'esecuzione. L'utente si vede costretto ad intervenire continuamente per «legittimare» i file.
- Importantissimo l'aggiornamento delle definizioni, altrimenti senza "vaccino" non viene riconosciuto il virus. Generalmente l'aggiornamento è automatico e non va disabilitato.
- Un Antivirus **shareware** spesso hanno aggiornamenti limitati nel tempo, per averne un pieno e aggiornato uso bisogna acquistarlo.

5.2.2.2. INSTALLARLO SU TUTTI I SISTEMI

- Vista la funzione che ha l'antivirus dovrebbe essere installato su tutti i sistemi informatici.
- Tutti gli strumenti informatici potrebbero essere una fonte di lucro per il furto dei dati o come via per estorcere denaro.
- Le informazioni raccolte su uno strumento, personali o aziendali, potranno avere un grande valore non solo per il proprietario ma… anche a qualche truffatore.

5.2.2.3. AGGIORNAMENTO DEI SOFTWARE

- Il database delle **definizioni** dei virus va aggiornato continuamente in modo da garantire la sicurezza delle informazioni.
- Un antivirus viene aggiornato anche **in seguito** alla creazione dei malware.
- E' opportuno aggiornare anche i software installati sul computer (applicativi, sistema operativo, plugin, browser web) perché risolvono eventuali bug o malfunzionamenti, evitare problemi di incompatibilità che un programma vecchio potrebbero non affrontare

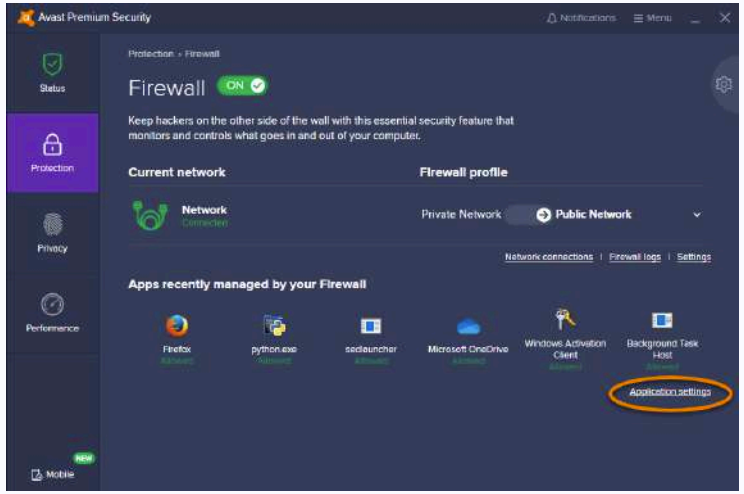


5.2.2.4. ESEGUIRE/PIANIFICARE SCANSIONI SPECIFICHE

- Oltre alla scansione automatica è bene scansionare manualmente cartelle e file sospetti.
- In modo particolare è bene farlo quando si scarica un file compresso, un allegato alla mail. Si può fare una **scansione mirata** a una **scansione** totale **periodica,** niente di file e cartelle.
- le modalità di **pianificazione** variano a seconda del software utilizzato.
- In molti casi la scansione mirata si fa con il tasto destro del mouse una volta selezionato l'oggetto (file, cartella, disk).

5.2.3.1-2. RISOLUZIONE E RIMOZIONE/QUARANTENA

- Se l'antivirus non può eliminare un file sospetto lo mette in quarantena, cioè lo conserva per un certo periodo in attesa della soluzione del problema (aggiornamento). Al termine del tempo stabilito, in assenza di soluzione, lo elimina.
- Di fronte ad un problema/sospetto l'antivirus **suggerisce** l'eliminazione o la messa in quarantena. Attraverso una finestra di dialogo viene presentata l'opzioni all'utente.

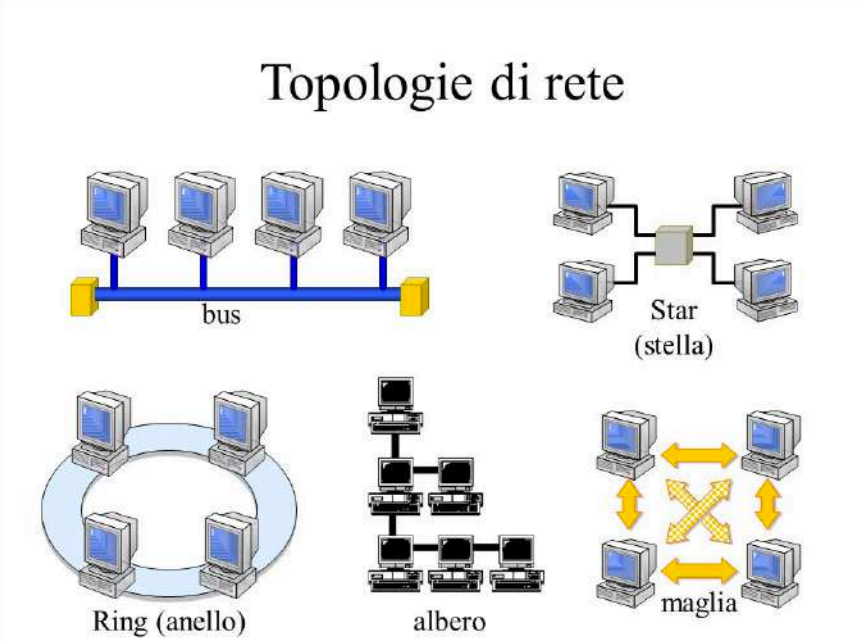


5.3. LA SICUREZZA IN RETE

MODULO 5 - UNITÀ 3

5.3.1.1. LE RETI INFORMATICHE

- Per rete informatica si intende un insieme di computer connessi tra di loro per condividere risorse o accedere a periferiche condivise.
- Prima le reti erano solo accademiche o professionali, ora sono domestiche; prima servivano i fili, ora le onde (wireless)
  - **LAN** (Local **AREA NETWORK**) più computer collegati in un'area ristretta da un cavo di rete (es. scuola). Possono essere:
    - a rete a stella,
    - a hub,
    - a bus
  - **WLAN** se il collegamento è wireless
  - **WAN** (**WIDE AREA NETWORK**) più reti collegate tra di loro attraverso una linea telefonica (internet)
  - **VPN** (**VIRTUAL PRIVATE NETWORK**) rete privata che usa un sistema di trasmissione pubblico, ma l'accesso non è pubblico.



5.3.1.2. SICUREZZA NELLA CONNESSIONE DI RETE

- Ogni sistema operativo mostra il tipo di rete disponibili (LAN o wireless).
  Il fatto che il computer sia collegato alla rete determina un problema di sicurezza. I rischi possono essere diversi:
  - gli accessi possono essere monitorati attraverso i **file di log** della rete e quindi c'è una potenziale **limitazione della privacy**;
  - **accesso non autorizzato** alla rete di uno che ha rubato le credenziali o una rete poco protetta dal firewall
  - **attacchi di malware** che si diffondono quasi esclusivamente nella rete
  - la rete wireless permette **accessi** anche se **non** si è direttamente **visibili** all'interno della rete. Per questo va sempre protetta da password

5.3.1.3.A. AMMINISTRATORE DI RETE RUOLO E COMPITI

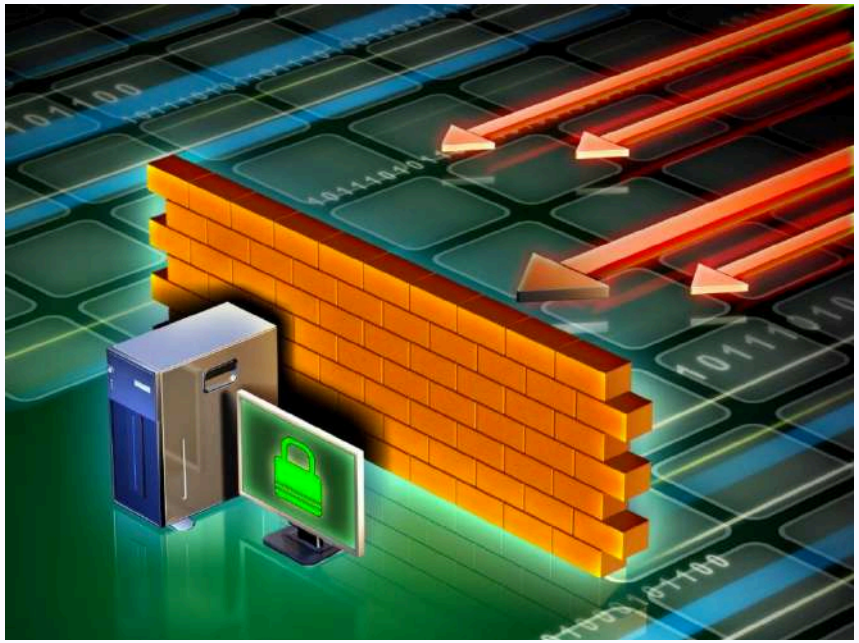
- I compiti dell'Amministratore di rete sono quelli di gestione, amministrazione e controllo:
  - assegna gli account di accesso agli utenti o ai dispositivi.
  - gestisce le credenziali di autenticazione agli utenti.
  - attribuisce i "privilegi", cioè le operazioni che un utente può compiere.
  - può precludere l'accesso ai risorse o periferiche, a che gli intenti scarichino file dalla rete.
  - controlla la sicurezza del sistema e ne aggiorna le misure di sicurezza.

5.3.1.3.B. AMMINISTRATORE DI RETE RUOLO E COMPITI

- Altri I compiti dell'amministratore di rete:
  - assegna gli account di accesso agli utenti o ai dispositivi.
  - gestisce le credenziali di autenticazione agli utenti.
  - verifica degli aggiornamenti deve essere periodica per assicurarsi che siano state rilasciati. aggiornamenti/novità
  - gestisce gli attacchi da malware sulla rete che amministra.
  - tiene sotto controllo il traffico di rete per vedere anomalie, stranezze che prefigurano attacchi da malware, accessi abusivi o uso non consentito della rete e della strumentazione.

5.3.1.4.A. LE FUNZIONI E I LIMITI DEL FIREWALL

- Il firewall (mura tagliafuoco) è un qualsiasi mezzo che filtra o blocca gli accessi alla rete in ingresso e in uscita.
- Permette un altissimo grado di protezione in quanto blocca ogni accesso non autorizzato.
- Se mal configurato potrebbe bloccare anche connessioni sicure, impedendo ogni operazione o non ritenerla affidabile.

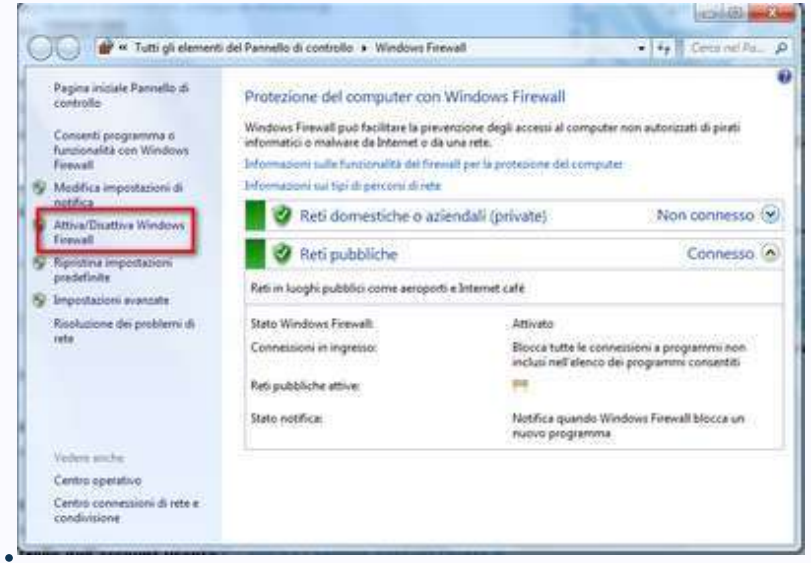


5.3.1.4.B. ATTIVARE O DISATTIVARE FIREWALL PERSONALI

- Esistono anche firewall personali, software da installare su un singolo pc che filtra gli accessi sospetti o blocca i tentativi di inserimento dall'esterno di programmi presenti sul computer.
- Anche in questo caso va configurato in modo da permettere ogni servizio di rete, di accesso a tutti i programmi non sospetti.

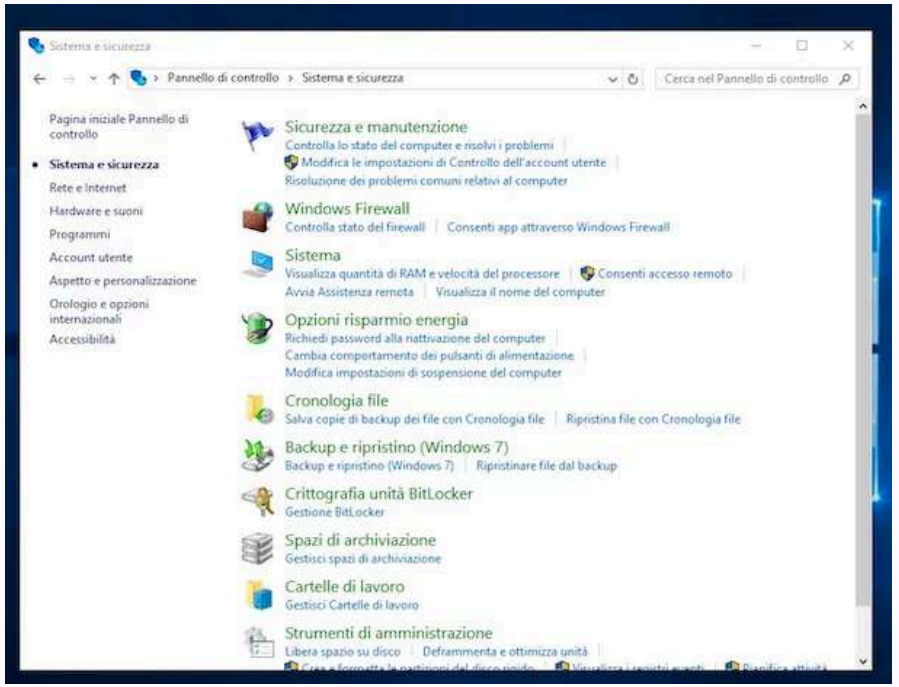
5.3.1.5.A. ATTIVARE WINDOWS FIREWALL

- **Start**
  - > **Pannello di controllo** > **Sistema di Sicurezza** > **Windows Defender Firewall**
    - > **Personalizza Impostazioni per ogni tipo di rete**
    - > **Attiva/disattiva Windows Firewall.** (potrebbe richiedere password di amministratore)
- si può attivare la protezione per diversi tipi di percorsi
    - > **Impostazioni di rete privata**
    - > **impostazione di rete pubblica**
    - > **ok**
- si possono bloccare tutti i programmi anche se consentiti prima
    - > **"Blocca tutte le connessioni in ingresso comprese incluse quelle nell'elenco delle app consentite"**



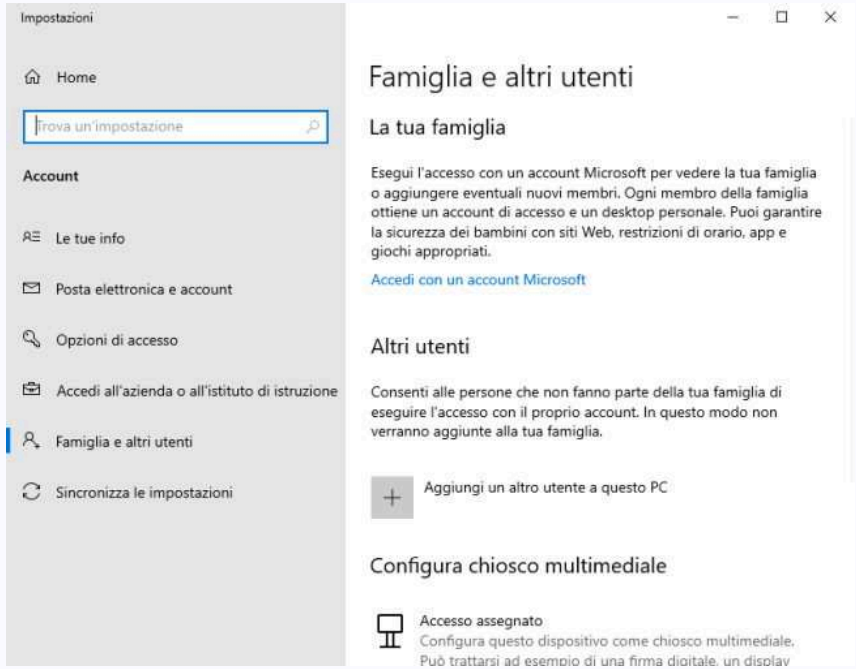
5.3.1.5.B. DIS/ATTIVARE WINDOWS FIREWALL

- Via alternativa:
  - > **Start** > **Pannello di Controllo** > **Sistema Windows**
- nella casella di ricerca: firewall
- > **Windows firewall** > **Personalizza impostazioni**
- --- come sopra (B)
- DISATTIVARE WINDOWS FIREWALL
  - dalla finestra: **Windows Firewall**
  - > **personalizza impostazioni** > **Attiva/disattiva Windows Firewall**
  - scegliere quale percosso disattivare > **ok**
- Andrebbero disattivate la maggior parte delle connessioni in ingresso per la sicurezza del PC. Per alcune potrebbero essere consentite le informazioni attraverso il firewall, impostando criteri specifici.



5.3.1.5.C. CONSENTIRE L'ACCESSO AD UNA APPLICAZIONE

- SERVIZIO IN AMBIENTE WINDOWS
  - > **WINDOWS Firewall**
  - > **App. consentite**
  - > **consenti App o funzionalità attraverso Windows Firewall**
  - > **modifica impostazioni** (da amministratore)
  - > **selezionare i tipi di rete con cui si desidera consentire la comunicazione**
  - > **ok**



5.3.2.1.A. TIPI DI SICUREZZA PER RETI WIRELESS

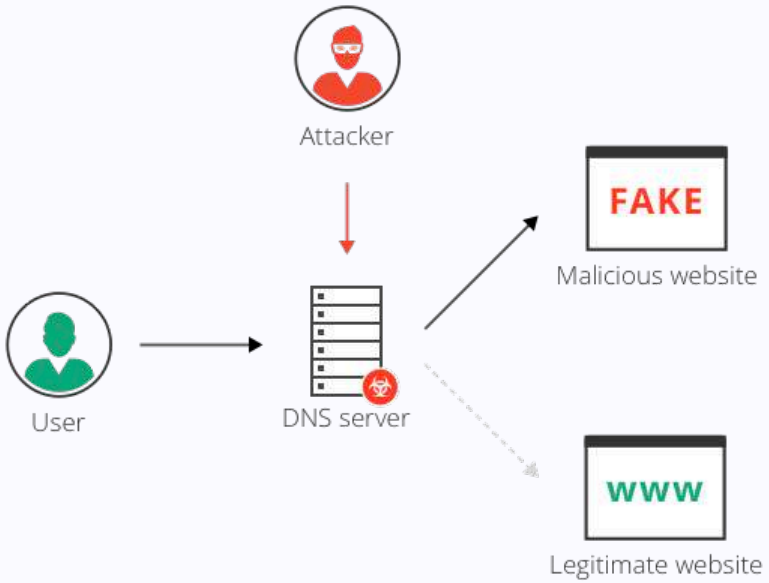
- Pur proteggendo le reti wireless, comunque la rete wireless può essere intercettata da chi non è autorizzato, perfino spiata. Ciò rende necessario lo scambio dei dati sia crittografato.
- Ci sono due tipi di protezione:
  - il **WEP** (Wired Equivalent Privacy)
  - il **WPA** (wifi Protected Access)
    - differenziano per la robustezza dell'algoritmo di crittografia usata a favore del secondo. Entrambi hanno una password, quella del Wpa in più ha una *passphrase* (stringa di caratteri più lunga, anche con senso compiuto)
  - il **WPA2** è più efficace perché usa il protocollo di crittografia **CCMP**

5.3.2.1.B. TIPI DI SICUREZZA PER RETI WIRELESS

- Ci può essere una protezione attraverso una lista di accesso che permette accesso alla rete se in possesso di un indirizzo **Mac** (**Media Access Control**), l'indirizzo univoco dato dal produttore che identifica il device.
- **SSID** è la stringa di testo con cui la rete wifi indica la propria identità agli utenti.
- Anche se il nome viene nascosto non vuol dire che la rete non sia individuabile e violabile.

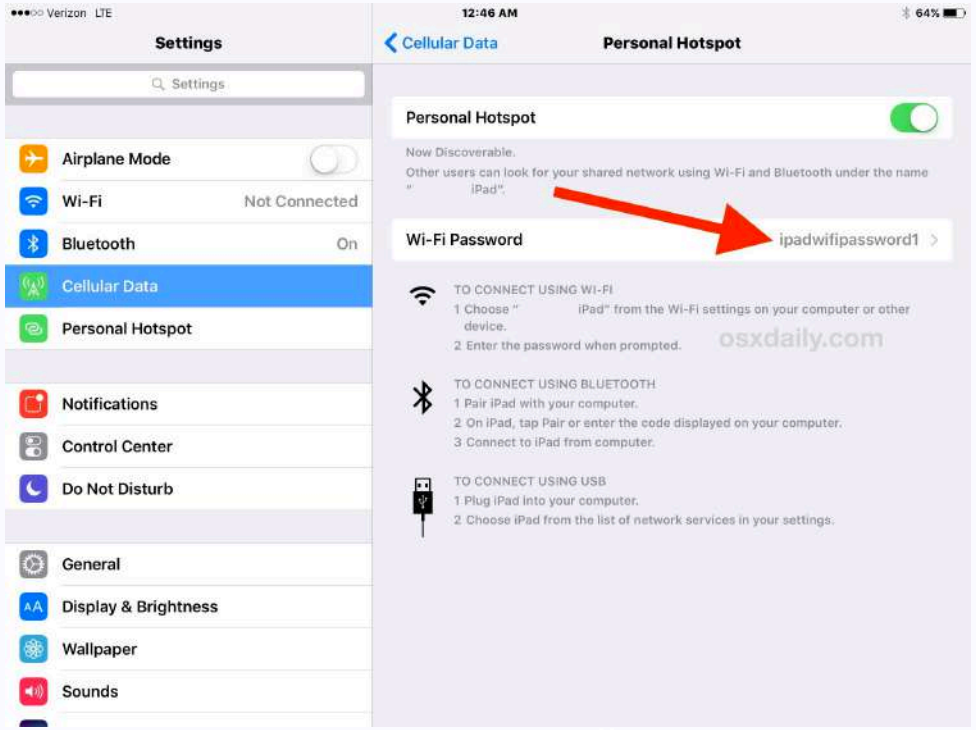
5.3.2.2. POSSIBILI ATTACCHI SU RETI WIRELESS

- Una rete non protetta può essere a rischio di intercettazioni (**eavesdropping**) mettendola di fronte a diversi rischi:
  - prendere conoscenza delle informazioni comunicazioni, modificarle, o inviare comunicazioni come se fosse il vero mittente (**Man in the Middle**), chiedere informazioni sensibili.
  - network **hijacking** cioè dirottare le comunicazioni verso siti diversi da quelli che l'utente vorrebbe visitare, cioè **un malware in grado di modificare le impostazioni del browser,** senza autorizzazione, per fare sì che l'utente venga rediretto su siti Web che non aveva intenzione di visitare.



5.3.2.3. COSA E' UN 'HOTSPOT PERSONALE'

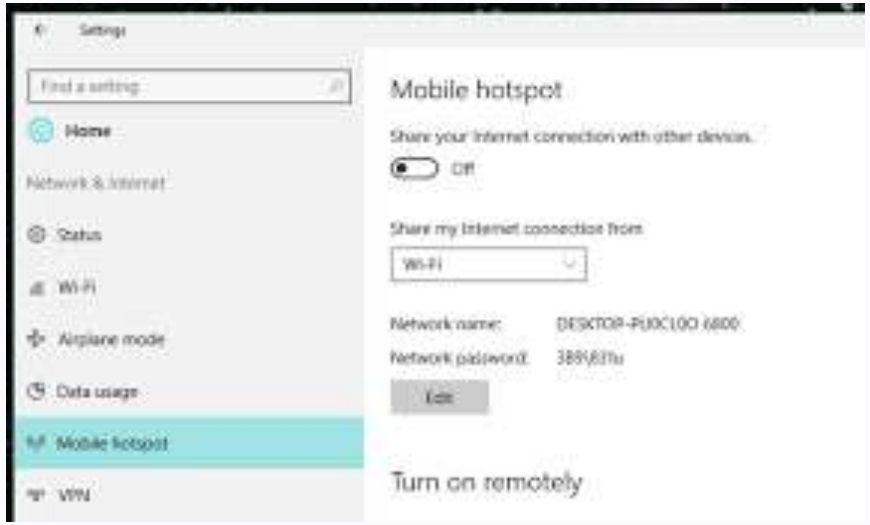
- Gli **hotspot** sono punti di accesso alla rete wireless, dei punti in cui è possibile una connessione a Internet aperta al pubblico.
- Per **hotspot personali** si indica un dispositivo che permette di condividere la connessione dati da un dispositivo mobile a dispositivi fissi o mobili purché a conoscenza delle credenziali di accesso e che abbia una scheda di rete wireless



5.3.2.4.A. ATTIVARE UN HOTSPOT SICURO

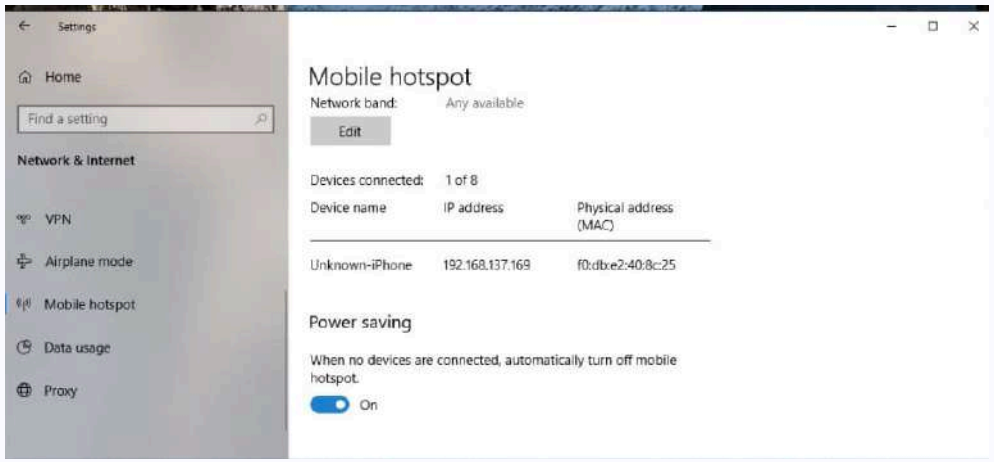
CONNETTERE DISPOSITIVI INFORMATICI

- Procedura se si è su un dispositivo con installato **Windows 10 Mobile**
  - > **Start** > **tutte le App…**
  - **Attivare** > **Condividi la connessione con altri dispositivi**
  - > **Impostazioni di rete e wireless/hotspot mobile** >
  - scegliere l'opzione Wi-fi o Bluetooth per la voce > **Condividi la connessione internet da...**
- Per configurare il nome della rete e impostare la password di accesso:
  - > **Modifica/Immetti un nuovo nome di rete e una password**
  - > **salva**



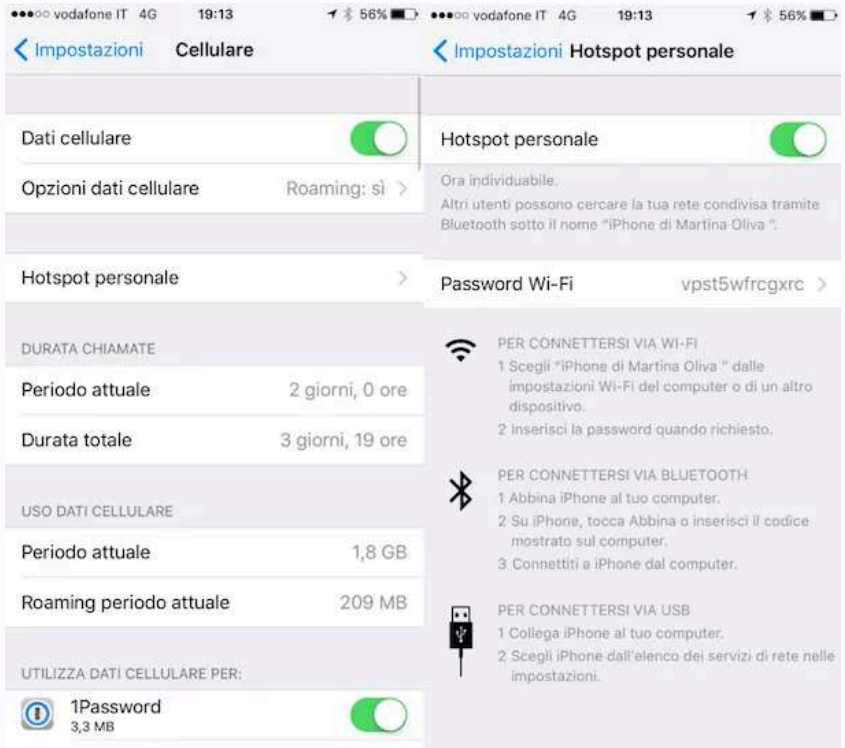
5.3.2.4.B. DISATTIVARE UN HOTSPOT SICURO

- > **Start** > **Tutte le App** > **Impostazioni/Rete e wireless/Hotspot mobile**
- > '**Disattivato**' alla voce: > **Condividi la connessione internet con altri dispositivi**
- DISPOSITIVO GENERICO
  - > **impostazioni del wifi**
  - > **selezionate la rete dal nome**
  - > **Inserire la password**
  - > **Connetti/Disconnetti**



5.3.2.4.C. DISATTIVARE UN HOTSPOT SICURO

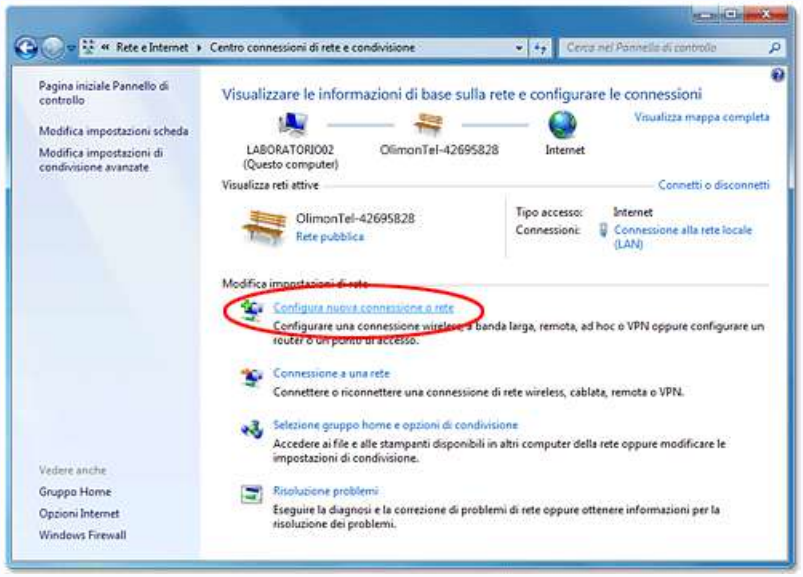
- **HOTSPOT PERSONALE SU IOS (iPhone, iPad)** > **Impostazioni** > **cellulare** > **hotspot personale** > **ON** > Password wifi (per impostare la password di accesso alla rete)
- **HOTSPOT IN ANDROID** > **Impostazioni** > **Wireless e Rete** > **Altro/Tethering hotspot** portatile configura hotspot wifi > Assegnare un nome alla rete (SSID) e impostare una password per la connessione > **salva**
- una volta configurato per abilitarlo > **tethering hotspot portatile** > spunta **Hotspot wifi portatile**



5.3.2.4.D. DISATTIVARE UN HOTSPOT SICURO

CONNESSIONE SU WINDOWS

- la presenza di una scheda di rete permette di ricevere segnali dai punti di accesso wireless.
- Nell'area di notifica (in bassa ad a) un'icona mostra la connessione wireless. Tasto dx del mouse apre una finestra con le rete e la potenza del segnale.
  Mantenendo il cursore, nella rete un'etichetta mostra il tipo di sicurezza attiva..
  Inoltre apparirà il pulsante: connetti un lucchetto chiuso evidenzia la necessità di una password
- Digitata la chiave d'accesso, il cambio di colore indica la connessione attiva.
- "**connetti automaticamente**" collega direttamente il pc una volta nel raggio del router. "**Disconnetti**"

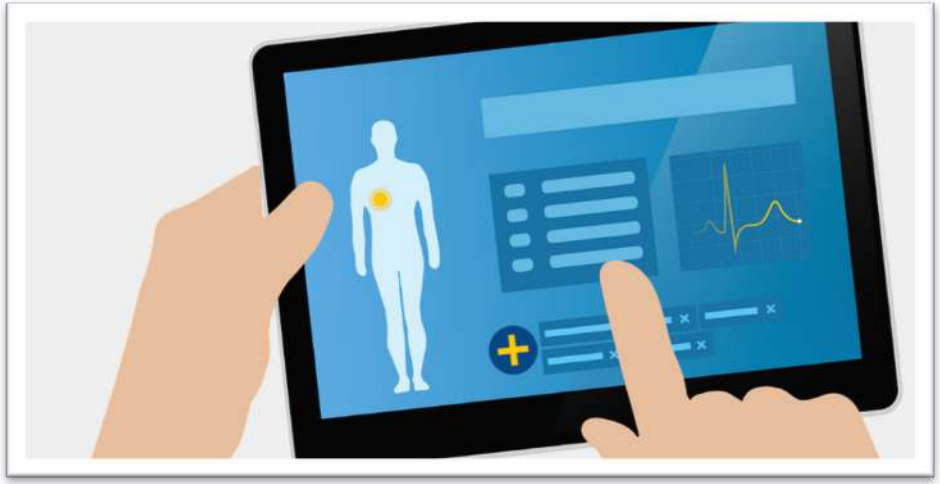


5.4. CONTROLLO DI ACCESSO

MODULO 5 - UNITÀ 4

5.4.1.1. PREVENIRE ACCESSI NON AUTORIZZATI AI DATI

- Per sicurezza è opportuno definire le procedure e i protocolli che permettono l'accesso ai dati solo a chi è autorizzato e per quanto gli compete.
- Nei database e ai programmi di gestione si può:
  - inserire username e password riconoscibile dal sistema con prerogative specifiche:
  - cifratura, con caratteri non intellegibili a chi non ha la chiave che decripta i dati.
  - **Pin** (**Personal Identifier Number**) per l'accesso viene utilizzato un codice numerico segreto legato all'identità dell'utente.
    Questo può essere associato in una autenticazione a più fattori: per l'acceso, oltre a username e password, si chiede di digitare codici inviati via SMS email.

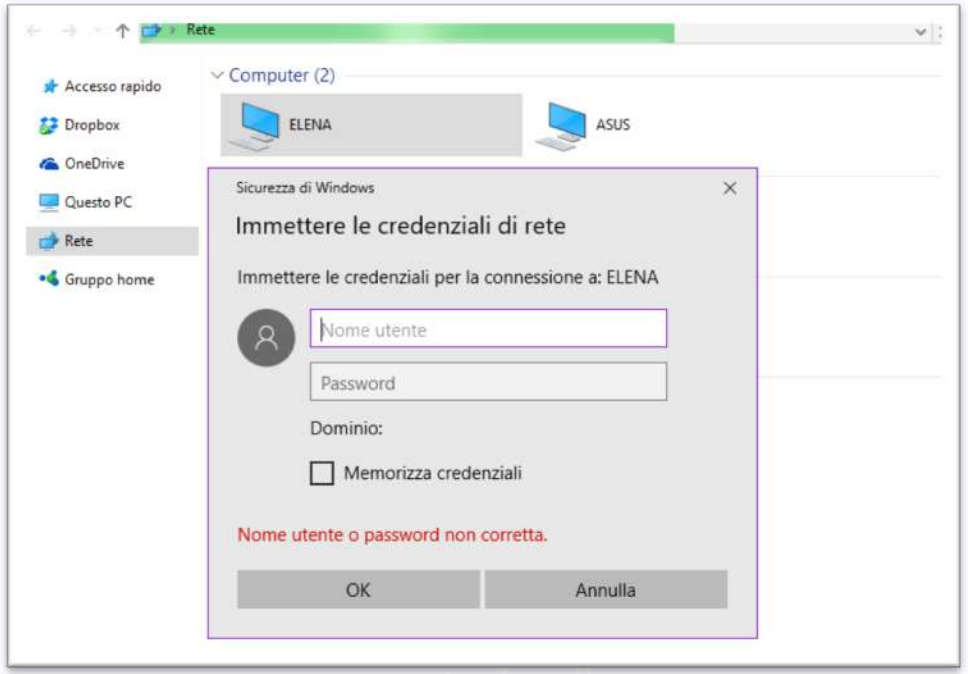


5.4.1.2. “ONE-TIME PASSWORD” E IL SUO UTILIZZO

- Una evoluzione dell'autenticazione a 2 fattori e la **one-time password**, o password di sessione. Questa ha una validità temporanea, da utilizzare 1 volta e per 1 operazione generata con un **token** (hardware specifico) è una password comunicata attraverso una via diversa rispetto a quella di comunicazione dei dati (computer).

5.4.1.3.4. ACCOUNT DI RETE

- Per l'accesso ad una rete l'amministratore deve attribuire un account di rete ad ogni utente e con esso i privilegi di azione.
- Al momento dell'accesso l'utente deve autenticarsi con nome utente (dato dall'amministratore) e dalla password (nota solo all'utente e al sistema informatico) Alla fine dell'utilizzo l'utente si deve disconnettere con i log-out, liberando la rete ed entrando che altri usino le sue credenziali.

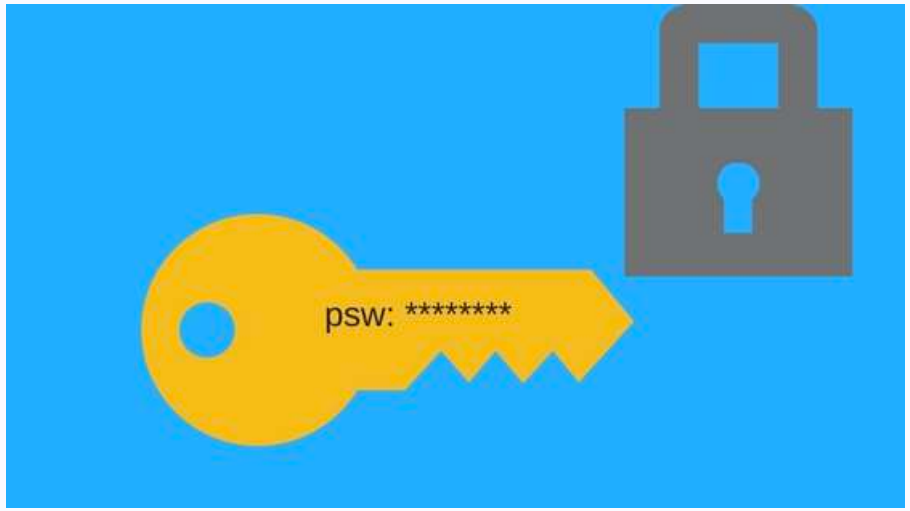


5.4.1.5. LA SICUREZZA BIOMETRICA

- Nell'ultimo periodo si sta facendo ricorso al riconoscimento biometrico, cioè alla capacità di alcuni strumenti di riconoscere dati fisici riconducibili all'utente:
  - impronte digitali
  - la voce
  - composizione dell'iride
  - geometria della mano
  - riconoscimento facciale

5.4.2.1-2. LA SICUREZZA DI UNA PASSWORD

- La password è un elemento di sicurezza perché permette l'accusa in rete, mia collega all'utente tutte le operazioni da lui compiute. Perciò la password non deve essere condivisa con altri. Inoltre deve essere rinnovata periodi-camente.
- La password sicura deve essere ALMENO:
  - 8 caratteri e una cifra
  - un simbolo (carattere non alfanumerico)
  - se il sistema è 'case sensitive' (riconosce maiuscole e minuscole) inserire 1 maiuscola.
- Si sconsigliano:
  - nomi propri, parole di senso compiuto
  - numeri riferibili ad una data coerente
  - sequenze di caratteri riconducibili all'utente
- Utilizzando più servizi di rete non utilizzare la stessa password, violata una volta può creare danni su più pronti
- La memorizzazione della password va usata con parsimonia perché il furto del device non comporti anche il furto delle password..

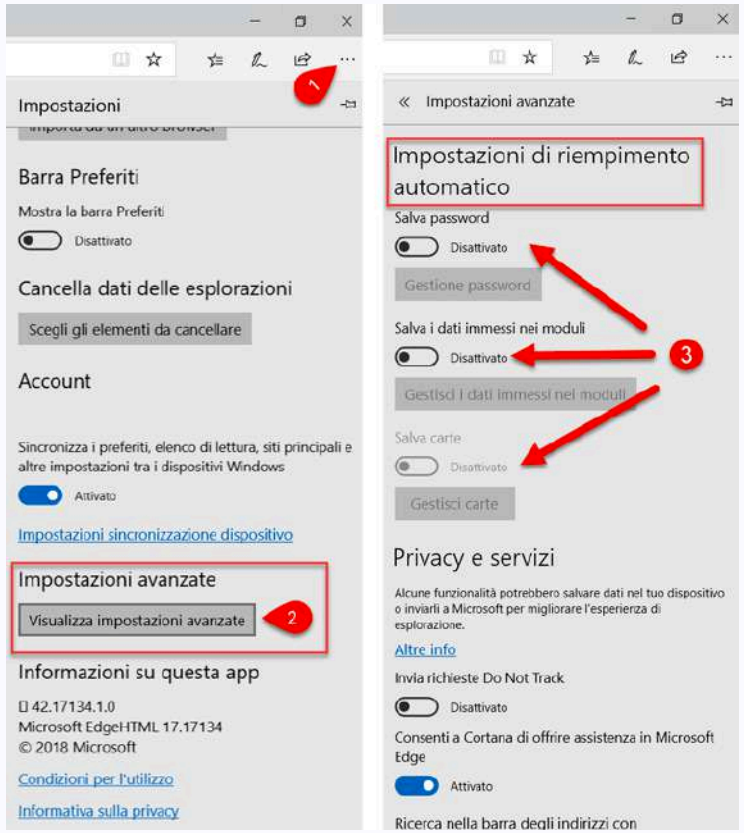


5.5. USO SICURO DEL WEB

MODULO 5 - UNITÀ 5

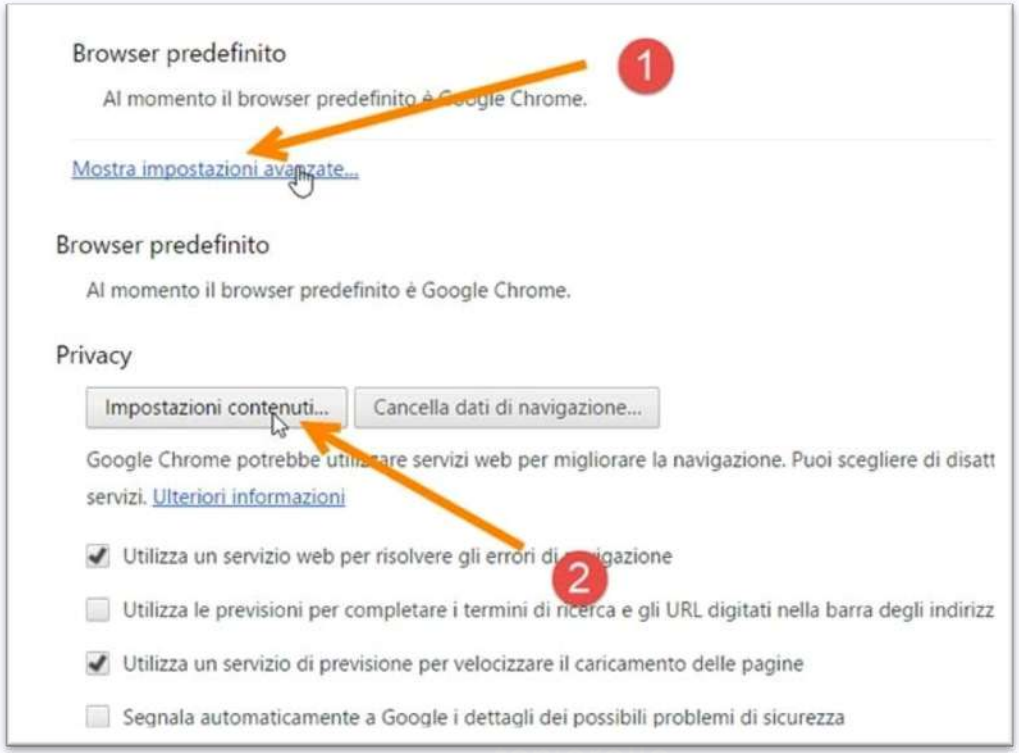
5.5.1.1. COMPLETAMENTO/SALVATAGGIO AUTOMATICO

- Uno dei rischi più comuni quando si inviano date all'interno dei moduli presenti sulle pagine web è rappresentato dal completamento e salvataggio automatico.
- Il browser riconosce i dati che si stanno per digitare quindi completa automaticamente e propone di scegliere i dati guai inseriti in precedenza.
- Tutto ciò rappresenta un rischio perché si può inserire un dato sbagliato.
- Altro rischio è quando lo stesso pc è utilizzato da più utenti che fanno le stesse operazioni. In questo caso andrebbe disabilitata questa funzione.



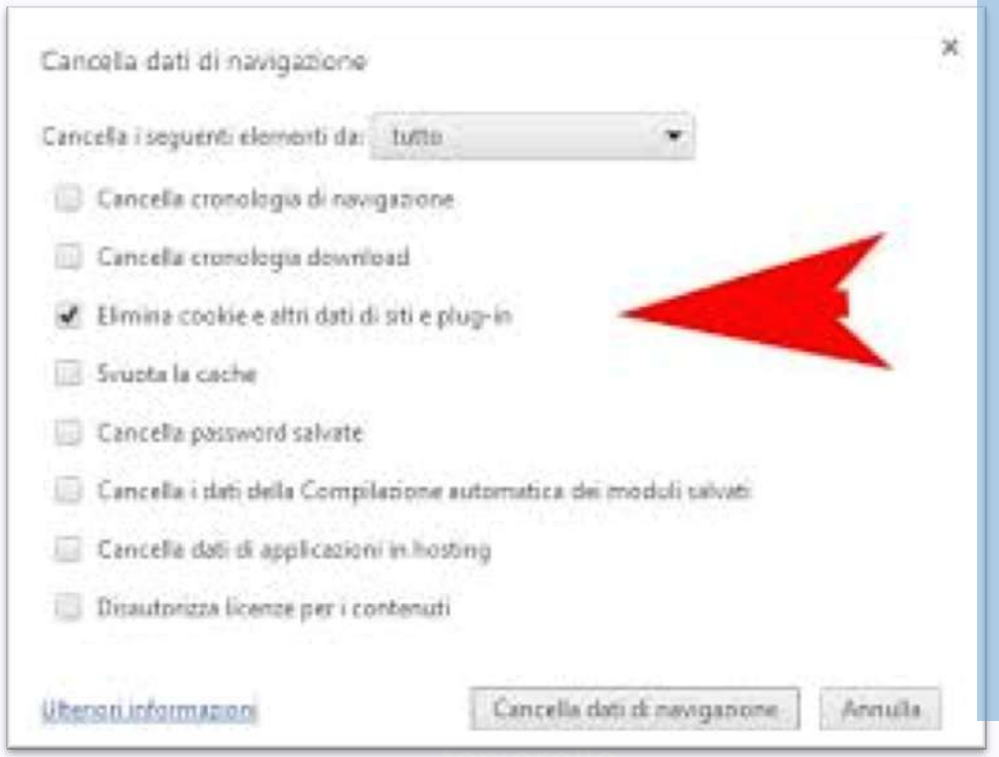
5.5.1.2. ELIMINARE DATI PRIVATI DAL BROWSER

- I **Cookie** (biscottini) sono piccoli file che si scambiano tra il sito e il browser, dove si registrano i dati di navigazione nel sito che hai in via.
- I cookie servono per il web marketing, il commercio elettronico-perché profila le pagine, i siti visitati e le ricerche fatte. Chi gestisce i siti può predisporre le pagine (pubblicità se pensa possano interessare.
- L'invio deve essere "ancora autorizzato dall'utente quando aiuta il sito e si registra a un sito quando accetta le condizioni generali di utilizzo.



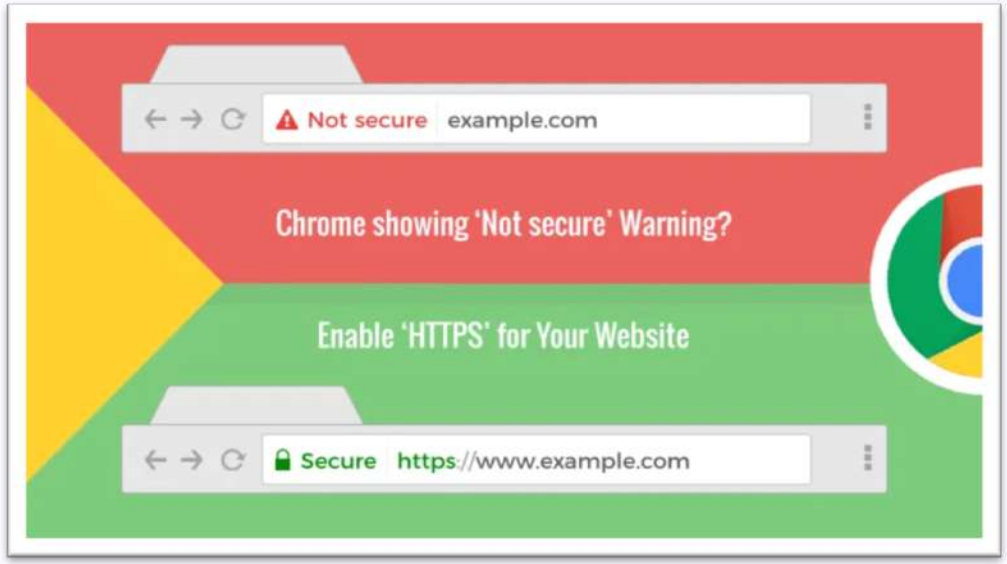
5.5.1.2.B. ELIMINARE DATI PRIVATI DAL BROWSER

- Il Garante della privacy dal giugno del 2015 ha resa obbligatorio per i siti ad informare dell'esistenza dei cortei e chiedere il Consenso all'utente se usa coatti di profilazione finalizzate all'invio di pubblicità.
- oltre ai Cookie, i dati inseriti e memorizzati, i browser conservano la cronologia dei siti e delle pagine visitate, sono conservati i file temporanei, file scaricate con applicazioni diversi dal browser, come Word e Pdf. Rimanendo in memoria possono essere eliminati.



5.5.2.1. SITI SICURI

- Per la navigazione sicura quando si devono effettuare operazioni sicure dove si inseriscono dati sensibili come banking online, acquisti,...
- Questi siti predispongono pagine sicure, cioè crittografata. Tali pagine nella barra degli indirizzi il nome del sito è preceduto da **https**, dove la "**s**" sta per "**secure**" e da un **lucchetto chiuso.**



5.5.2.2.A. CONFERMARE L'AUTENTICITÀ DI UN SITO

- Per valutare un sito web oltre alla sicurezza va tenuto presente anche:
  - il contenuto che non sia copiato,
  - le traduzioni "*translate*"
  - le notizie vecchie.
- E' bene controllare la validità dell'URL, se si tratta effettivamente ciò che si cerca, in alcuni casi c'è qualche leggera differenza nell'URL.
- Importante accedere nella pagina del "chi siamo" di un sito in modo da verificare le informazioni sulla società e la persona che gestisce il sito (In caso di dubbio inviare una mail al contatto presente nella pagina).
- E' bene anche verificare a chi è registrato il nome del dominio attraverso i servizi *who-is* disponibili sul web.

5.5.2.2.B. IL CERTIFICATO DIGITALE

- La sicurezza dei dati trasmessi sul web è resa più solida con un certificato digitale, una sequenza di bit rilasciata da un ente terzo che definisce una identità al sito. L'Ente terzo è un'**Autorità di Certificazione** (CA) che rilascia questo documento elettronico che associa un soggetto ad una chiave pubblica. Il certificatore verifica l'associazione tra una chiave pubblica e l'utente e la sua chiave privata.
- Per vedere il certificato cliccare sull'icona del lucchetto nella barra degli indirizzi e contiene:
  - il soggetto che emette il certificato
  - a chi appartiene il certificato (sito)
  - la data di scadenza (1- 2 anni)

5.5.2.3 COSA E' IL PHARMING

- Il **Pharming** è una tecnica di dirottamento di un utente su un sito donato, di fatto quasi identico all'originale. L'inganno può avvenire attraverso un malware o manomettendo il server DNS del provider senza che l'utente se ne accorga (**phishing**)
- I siti clonati non hanno pagine sicure (https).
- Nella maggior parte dei casi si tratta di siti bancari/portali a e. come e.commerce.
- Nell'inserire i dati sul sito quei dati vengono rubati.

5.5.2.4. CONTROLLO DEL CONTENUTO

- Ci sono diversi software che permettono un controllo preventivo delle pagine, dei siti per filtrarli e bloccarne l'accesso a permetterlo solo se l'utente lo consente-
- Spesso si usa bloccare siti per tipologie specifiche (social, Giornali online, Giochi,...), o che permettono di scaricare file; creare un ambiente di navigazione protetto.

  Funzionano attraverso una **blacklist**.

5.5.2.4.B PARENTAL CONTROL

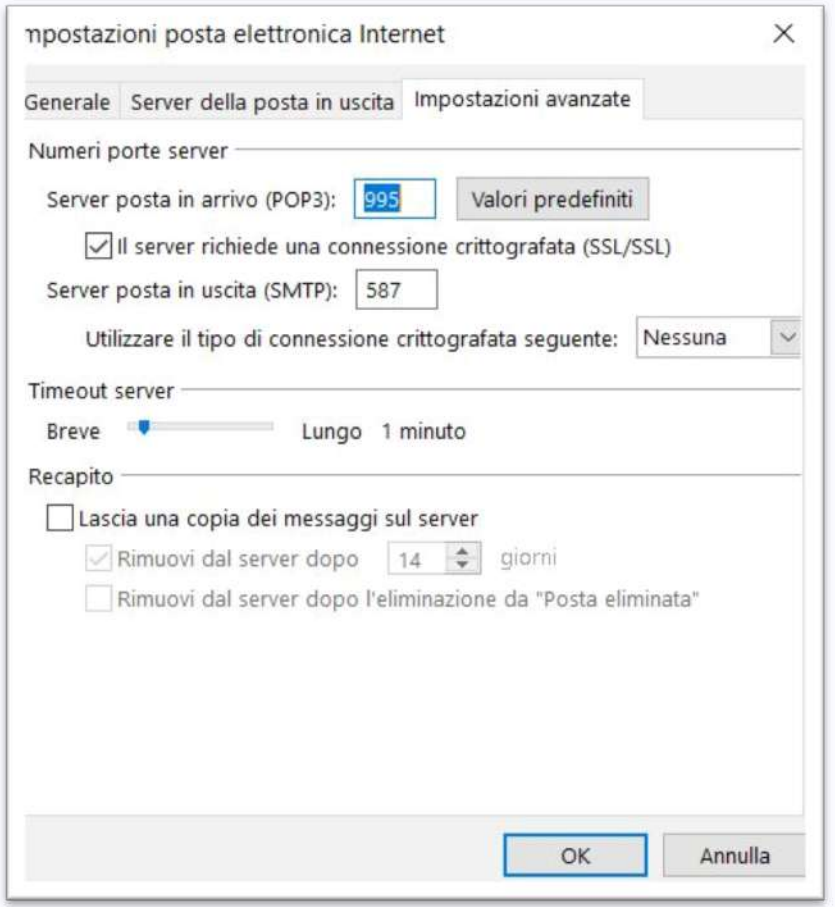
- Su vari Sistemi Operativi c'è il **Parental control:**
- **barra notifica** - cliccare sull'icona **Sicurezza Windows** (a forma di scudo) – seleziona: **opzioni famiglia'** - visualizza **Impostazioni famiglia.**
- Nel sito **Microsoft** - cliccare su **«creare un gruppo di account della famiglia»** - eseguire l'accesso con un account Microsoft (Outlook, hotmail, msn, ...) > **Reinventa l'esperienza familiare** - scegliere tra:
  - **Membro** (figlio)
  - **Organizzatore** (genitore)
    Gli organizzatori possa cambiare le impostazioni per verificare l'attività online
- Restrizioni di contenuto anche con report settimanali
  - **tenere traccia degli acquisti** > **Altre opzioni**> **spese**

5.6. COMUNICAZIONI

MODULO 5 - UNITÀ 6

5.6.1.1. DE/CIFRARE UN MSG POSTA ELETTRONICA

- I servizi di rete legati alla comunicazione, cioè posta elettronica e reti social presentano dei seri rischi.
- È possibile citare i messaggi utilizzando apposite estensioni all'interno dei client di posta elettronica (**Outlook, Thunderbird, Evolution**) che cifrano le mail automaticamente.
- Anche per i gestori di posta elettronica online è prevista la cifratura.



5.6.1.2. LA FIRMA DIGITALE

- La **firma digitale** si basa sulla crittografia a chiave pubblica è ha lo stesso valore di una firma cartacea, con lo stesso valore legale.
- Da non confondere con la scansione della firma autografa
- Inoltre garantisce:
  - **autenticità**, sicurezza della provenienza;
  - **integrità**, non si può modificare il contenuto del documento per attribuirlo ad altri;
  - **non ripudio**, non si può negare di averlo firmato.
- Il funzionamento è dovuto agli **algoritmi di Hash**.

5.6.1.3. MESSAGGI FRAUDOLENTI O INDESIDERATI E SPAM

- L'invio di messaggi contenente **spam** è detta **spamming**. Si tratta dell'invio di mail contenenti messaggi fraudolenti, con la richiesta di denaro, a link che assicurano guadagni facili o continue offerte pubblicitarie.
- **Origine del termine Spam (la carne in scatola dei Monthy Python):** https://youtu.be/Gxtsa-OvQLA

5.6.1.4-5. CARATTERISTICHE DEL PHISHING

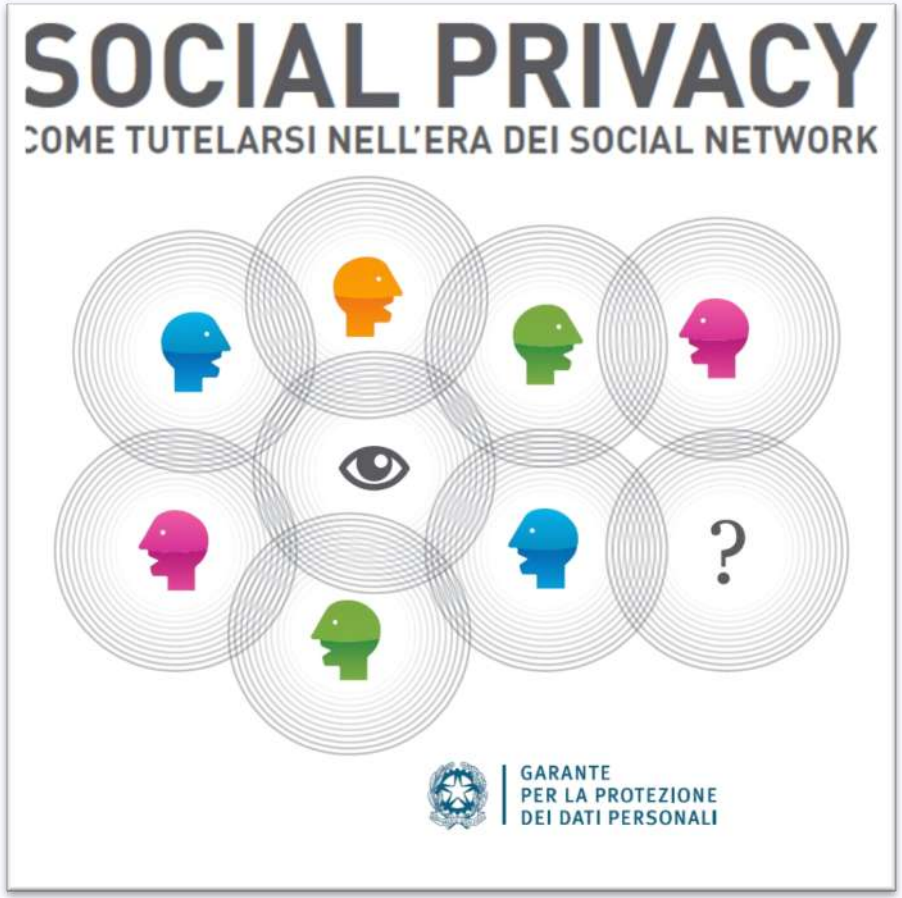
- La posta elettronica è il mezzo più diffuso per indirizzare a siti fasulli (graficamente uguali all'originale). Spesso chiedono di collegarsi al sito e resettare password o inserire dati "sensibili" che possono essere usate per fini fraudolenti.
- Il **phishing** può essere denunciato alle associazioni dei consumatori o alle autorità preposte come la polizia postale. Il **phishing** è una truffa e come tale va denunciata. I colpevoli possono essere individuati analizzando le mail, specie se abbastanza numerose.

5.6.1.6. RISCHI DELLA POSTA DEL PHISHING

- Come già evidenziato in precedenza le mail, con i loro allegati, possono essere un ricettacolo di malware, file eseguibili a documenti con macro. È bene non aprire file sospetti, poco chiari o provenienti da sconosciute, fare quindi attenzione agli avvisi che mostrano i file all'apertura.

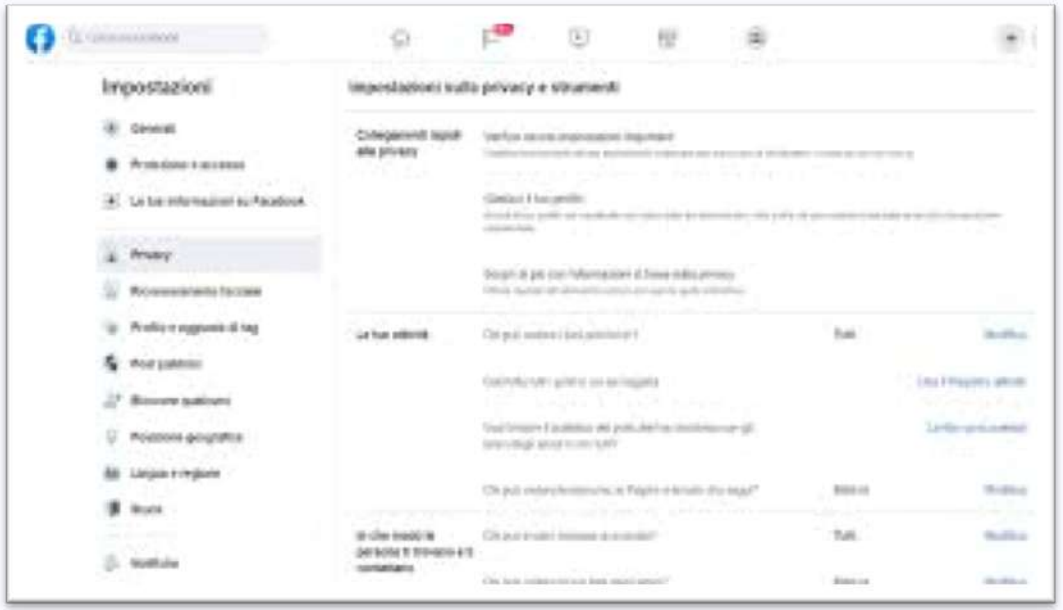
5.6.2.1. NON DIVULGARE SUI SOCIAL INFORMAZIONI SENSIBILI

- La leggerezza più comune che si commette sui Social è quello di divulgare con leggerezza informazioni riservate, personali, che permettono l'identificazione dell'utente anche a chi non fa parte dei propri contatti. Si mette a rischio la sicurezza della persona e quella informatica.



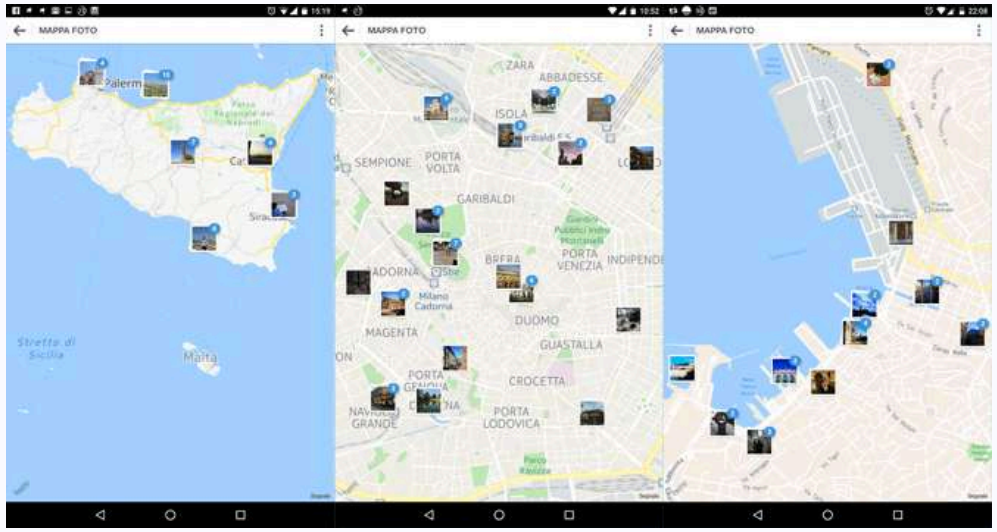
5.6.2.2. VERIFICARE LE IMPOSTAZIONI DELL'ACCOUNT SOCIAL

- Per garantire la riservatezza delle informazioni sui Social è bene verificare le importazioni del proprio account, in particolare per ciò che riguarda la riservatezza delle informazioni condivise e la posizione fisica dell'utente attraverso il Gps (presente nel Mobile).



5.6.2.3. APPLICARE RISERVATEZZA DELL'ACCOUNT

- Ogni Social permette di applicare delle impostazioni di riservatezza alle informazioni (riservatezza dell'account) e alla propria posizione (geolocalizzazione)
- Quindi dalle impostazioni si possono configurare le seguenti opzioni:
  - nascondere/visualizzare informazioni personali
  - nascondere/visualizzare post, notizie, contenuti
  - nascondere/visualizzare immagini e filmati
  - abilitare e disattivare la condivisione della propria posizione.
- Alcune importazioni si possono condividere solo con gruppi di utenti con credenziali progressive.*
- Opportuno impedire l'accesso alle nostre informazioni a chi non è presente nei propri contatti.



5.6.2.4. RISCHI POTENZIALI NELL'USO DEI SOCIAL

- Oltre quelli legati alla privacy, l'uso dei Social comporta altri rischi come:
  - **Cyber bullismo**: comportamenti fortemente lesivi della dignità delle persone. Le conseguenze a volte possono estreme.
  - **Adescamento**: (**grooming**): utilizzando i Social malintenzionati con false identità possono adescare altri utenti
  - Divulgazione dolosa di informatori personali.
  - false identità
  - Invio di link e messaggi fraudolenti.

5.6.2.5 DENUNCIA DI USI E COMPORTAMENTI NON APPROPRIATI

- Le vittime di chi fa usi non adeguati dei Social o le vittime di comportamenti inap-propriati da parte di altri utenti sulla rete è possibile denunciare il fatto a chi gestisce il servizio, perché rimuova l'account associato all'utente scorretto molestatore.
- In caso di "offese" a più gravi si può denunciare alla Polizia postale perché ci possono essere come guerre penali.

5.6.3.1. VULNERABILITÀ DI SICUREZZA PER IM

- La **Messaggistica Istantanea** (**IM**) presenta grosse vulnerabilità nel campo della sicurezza informatica:
  - propagazione malware con i file condivisi
  - accesso da **backdoor**
  - accesso ai nostri file da parte di non autorizzati
  - intercettazione delle informazioni trasmesse (**eavesdropping**)

5.6.3.2. VULNERABILITÀ DI SICUREZZA PER VOIP

- Anche la comunicazione Voip (Voice over IP), essendo un sistema che utilizza internet, trasportando la voce / video su un indirizzo Ip può essere oggetto di intercettazione.
- Per MI e VoIP ci sono Buone pratiche:
  - non accettare richieste di chat con sconosciuti
  - limitare la condivisione di informazioni
  - selezionare i file da inviare in base all'importanza (in caso ricorrere alla cifratura).

5.6.4.1. RISCHI DALLE APP DA "APP STORE" NON UFFICIALI

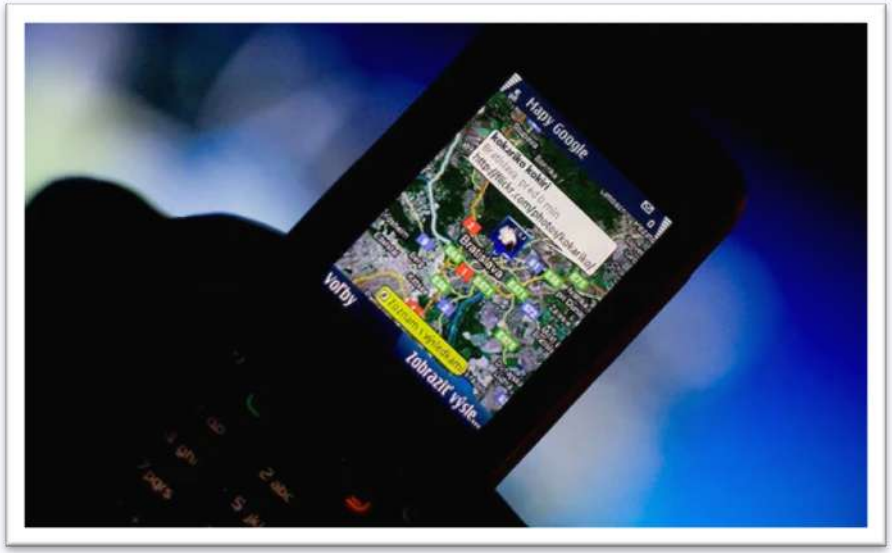
- Le App hanno determinato il successo dei dispositivi mobili perché semplici, utili, comode. Sono disponibili sugli App Store ufficiali dei principali produttori sia gratuite che a pagamento. Lo Store è garante della sicurezza di ciò che rende disponibile.
- Il ricorso a stare non ufficiali comporta una serie di rischi:
  - Presenza di malware
  - Utilizzo non necessario delle risorse (hardware, memoria, processore,...)
  - Accesso ai dati personali freschi sul dispositivo
  - Bassa qualità (potrebbe avere falle)
  - Costi nascosti non dichiarate.

5.6.4.2. AUTORIZZAZIONI DELLE APP

- Perché un'app funzioni correttamente richiede alcune autorizzazioni.
  - la posta richiederà l'accesso alla rubrica,
  - un'App di navigazione satellitare la Geolocalizzazione.
  - un'App di gestione delle immagini l'accesso alla Gallery
  - …
- Prima di installare un app bisogna usare coscienti di ciò che si autorizza.

5.6.4.3. LE APP POSSONO ESTRARRE INFORMAZIONI PRIVATE

- Le app, anche quelle Scaricate degli a degli a store ufficiali accedono sempre le informazioni contenute nel dispositivo estraendo dei dati dalla rubrica dei contatti, dalla cronologia della geo localizzazione dalla gallery presente in memoria.
- È pur vero che la negazione delle autorizzazioni potrebbero compromettere il completo utilizzo dell'app.
- È bene fare attenzione a cosa viene autorizzato quando si esegue l'app sul dispositivo. Una delle autorizzazioni più frequenti è relativa allo Stato e alla identità del telefono.



5.6.4.4. PRECAUZIONI IN CASO DI PERDITA DEL MOBILE

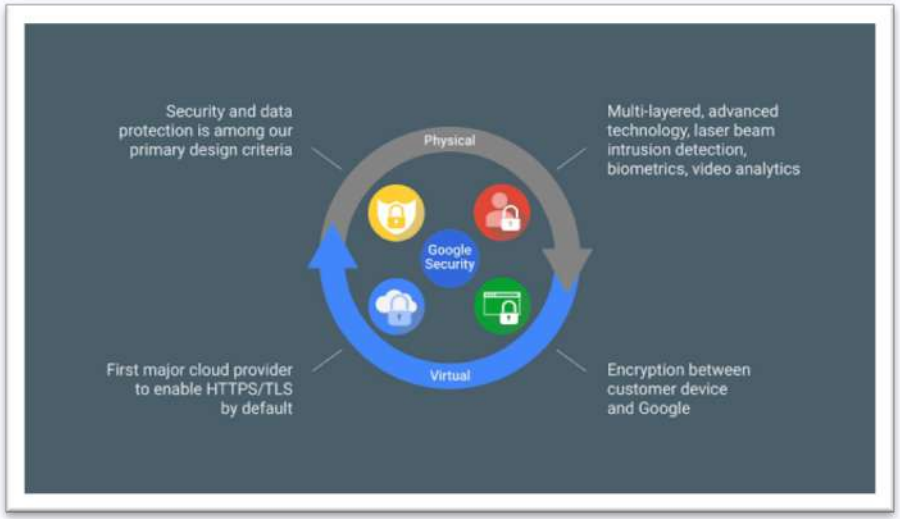
- In caso di smarrimento/furto del dispositivo Mobile ci sono delle tecnologie che sono state sviluppate per ridurre i rischi connessi al caso, come impedire l'accesso alle informazioni o di localizzare il dispositivo. Queste sono:
  - disattivazione remota, blocco per renderlo inutilizzabile
  - Eliminazione remota dei contenuti attraverso un altro device. I dati attraverso un Sms possono essere cancellati
- Queste funzionalità vanno configurate al primo utilizzo del dispositivo.

5.7. GESTIONE SICURA DEI DATI

MODULO 5 - UNITÀ 7

5.7.1.1. SICUREZZA FISICA DEL DEVICE

- La gestione più sicura per amministrare dati e garantirne la sicurezza e data dalla protezione dei dispositivi su cui sono stati memorizzati.
- Alcuni accorgimenti:
  - Non lasciarli incustoditi
  - Segnare sempre la collocazione fisica e i dettagli dei dispositivi.
  - Utilizzare i cavi antifurto
  - Controllare gli accessi ai dispositivi con sistemi biometrici.
- Questi primi accorgimenti valgono soprattutto per le aziende o per realtà dove c'è una condivisione di device o dove si devono memorizzare molti dati anche sensibili.



5.7.1.2. PROCEDURA PER COPIE SICURE

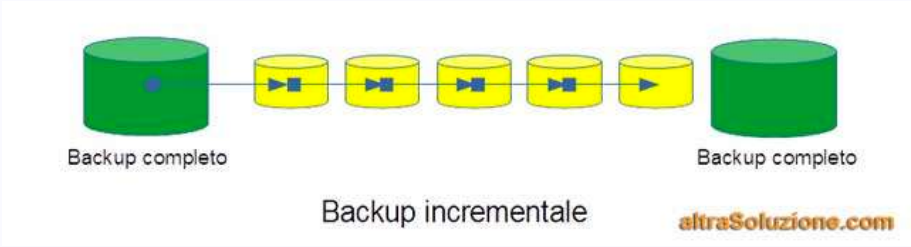
- Un'altra procedura per salvaguardare i dati e i programmi viene dai software che creano copie di sicurezza. Il fine è quello di recuperare i dati in caso di qualche imprevisto e comunque di non impedire il proseguimento del lavoro o il suo rallentamento
- L'efficacia di una copia di sicurezza sta anche nella sua periodicità regolare, particolarmente quando le modifiche e gli aggiornamenti del lavoro sono continui.

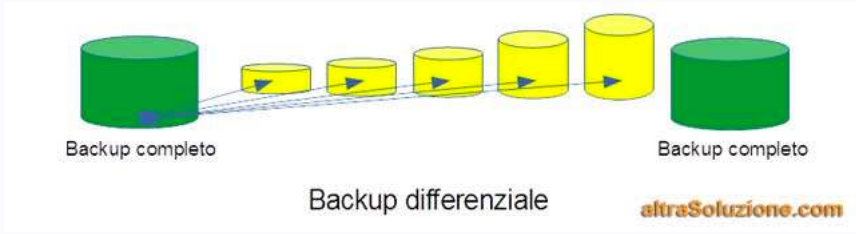
5.7.1.3.A. CARATTERISTICHE DELLA PROCEDURA DI COPIE DI SICUREZZA

- Le copie di sicurezza (o **backup**) dei dati presente su HD rigidi su computer va fatta su disk esterni in modo da ripristinare i dati in caso vengano persi.
- Vanno conservate in luogo sicuro e diverso da quello del computer.
- È possibile fare la compressione dei dati in modo da salvarli in un solo archivio risparmiando spazio, anche se i tempi di consultazione sono maggiori perché gli archivi vanno compressi e decompressi.
- La procedura di backup può essere anche programmata in modo da non interferire con il lavoro.

5.7.1.3.B. TIPI DI ARCHIVIAZIONE

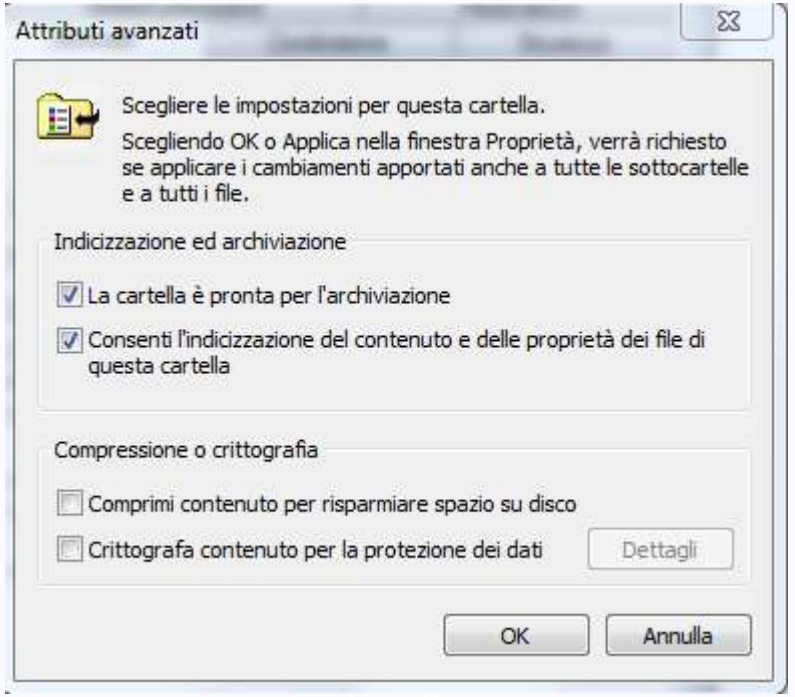
- Ci sono diversi tipi di archiviazione per un Backup:
  - **Completo**: consiste nella copia di tutti gli elementi selezionati
  - **Incrementale**, sono copiati soltanto gli elementi modificati rispetto al precedente backup incrementale o a quello completo, se non esistono altri backup differenziali successivi a quello completo.
  - **Differenziale**, sono copiati soltanto gli elementi modificati rispetto al precedente backup completo.
  - **Giornaliero**, copie che hanno l'attributo di 'archivio' nel giorno corrente
  - **Copia**: come un backup normale, ma non modifica "l'attributo" archivio
- Le copie di backup vanno fatte su HD esterni che variano da 500 Gigabyte a 8 TB. Inoltre è possibile usare le offerte degli archivi online, su computer remote, utili perché utilizzabili da qualsiasi luogo.





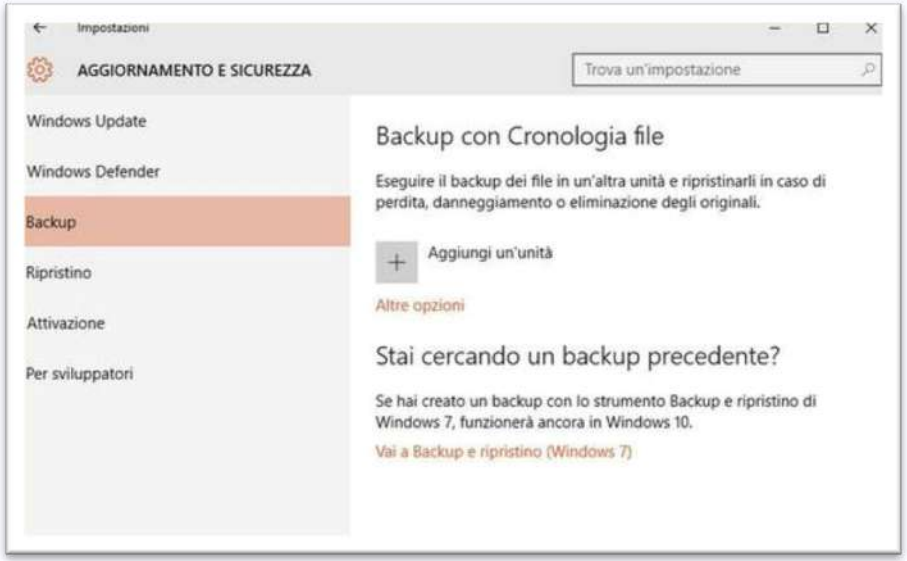
5.7.1.3.C. GESTIONE ATTRIBUTO DI ARCHIVIO

- Gli attributi sono metadati associati ad ogni file in modo da determinarne il comportamento e si visualizza dalle **Proprietà.**
  A – indica il file/cartella da archiviare e salvati da un backup
- **Gestione di un attributo Archivio su WINDOWS**
- > **esplora file**
- - tasto dx > **Proprietà**
- - scheda: **Generale** > **Avanzate**
- - nella finestra: **attributi avanzati**
- - spuntare: «**la cartella è pronta per l'archiviazione**» oppure «**il file è pronto per l'archiviazione**»
- > **ok**



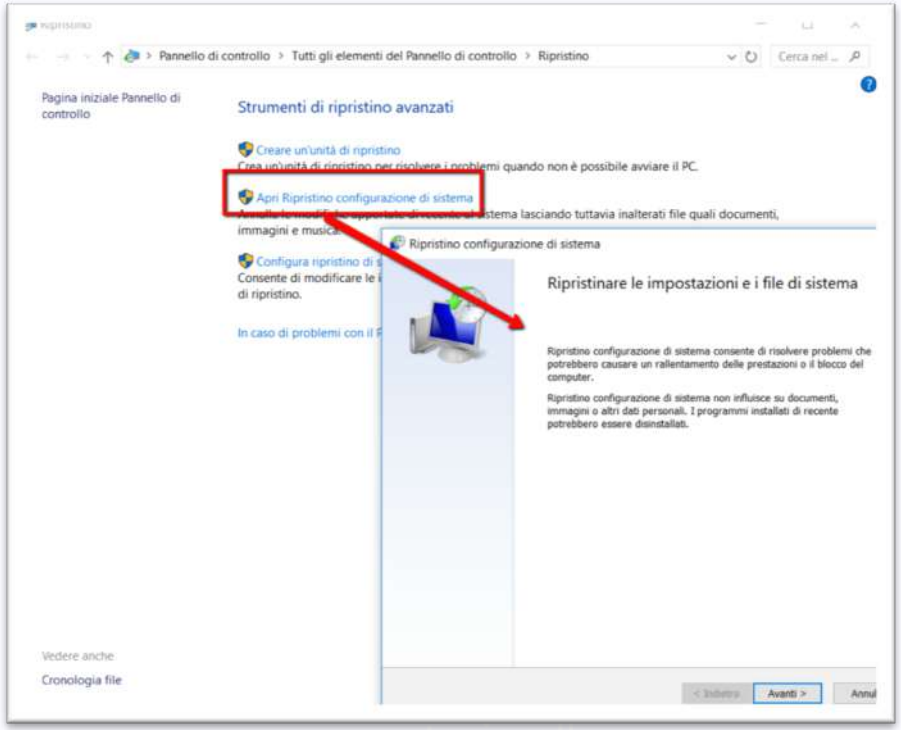
5.7.1.4. COPIA DI BACKUP SU SUPPORTO ESTERNO

- Per una copia di backup su **Window10** è possibile usare lo strumento **CRONOLOGIA:**
- A) > **Start**> **Impostazioni e sicurezza** > **backup** > **aggiungi una unità** - scegliere l'unità esterna o un percorso di rete su cui effettuare il backup
- B) strumento Backup e ripristino di **Windows 7** > **Start** > **pannello di controllo** > sistema e sicurezza > configura backup
- - indicare il dispositivo su cui fare il **backup** > **avanti**
- - Indicare se effettuare la selezione automatica (Archivio) o se manuale > **avanti** > impostare la frequenza (settimanale, giornaliera, mensile)
- Per specificare giorno e ora del backup da: **'Altre opzioni'** > **cronologia file** > **fine**



5.7.1.5. RIPRISTINARE I DATI DA BACKUP

- Per ripristinare i dati:
  - > **Start** > **impostazioni/sicurezza** > **Backup e ripristino** > **Ripristina file**
  - - la finestra mostra l'elenco dei backup con le relative informazioni (data, nome del computer, percorso di memorizzazione)
  - - scegliere la capra da ripristinare e una procedura guidata assisterà nell'operazione.
- In **Windows 10** si può effettuare il ripristino con lo strumento > **cronologia file.**
  - Nella ricerca scrivere: ***ripristinare file*** > Ripristina file con cronologia file
- - individuare il file e la versione da ripristinare> **Ripristina** (se nella stessa posizione) con tasto dx : > **ripristina in...** per posizione diversa



5.7.2.1. CANCELLAZIONE E DISTRUZIONE PERMANENTE

- La cancellazione dei dati o la formattazione dei dati rende gli stessi inaccessibili, non li elimina. Con appositi software si possono recuperare (*data recovery*) in tutto o in parte.
- La distruzione dei dati invece è permanente in quanto li elimina definitivamente non consentendone il recupero.

5.7.2.2. PERCHÉ ELIMINARE DEFINITIVAMENTE I DATI

- La distruzione sicura dei dati è una precauzione necessaria per proteggere i dati da minacce che possono venire da chi ne entra in possesso. Il semplice danneggiamento può portare al recupero.
- È bene renderli totalmente inaccessibili.

5.7.2.3. L'ELIMINAZIONE DEL CONTENUTO DEI SERVIZI

- I post e dati pubblicati sui **Social, blog** possono essere cancellati da chi li ha inseriti in rete.
- Come anche nei servizi cloud. **Non sempre, però, la cancellazione è immediata e permanente**. A volte difficile anche eliminare i dati i modo definitivo. Anche perché quei dati possono essere stati commentati, citati, condivisi. Ciò li rende ancora **presenti** nella rete.

5.7.2.4. METODI PER DISTRUGGERE I DATI

- Nel caso in cui un **supporto** è ancora **funzionante** e deve passare di mano è bene eliminare tutti i dati utilizzando software di cancellazione sicura.
- Se il **supporto non** è **funzionante** bisogna tenere presente che con particolari attrezzature (costose) si possono recuperare i dati, quindi è necessario renderli inservibili smagnetizzandoli con una calamita o danneggiandolo meccanicamente (martello o graffiando i dischi con cacciavite).