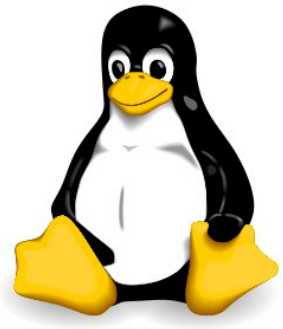
ECDL

LibreOffice
The Document Foundation

con software libero



Modulo 12

IT Security

(Sicurezza delle Tecnologie Informatiche)

ICDL
The Digital Skills Standard

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

Indice generale

SYLLABUS

Il presente modulo ECDL Standard Modulo 12 – Sicurezza informatica definisce i concetti e le competenze fondamentali per comprendere l'uso sicuro dell'ITC nelle attività quotidiane e per utilizzare tecniche e applicazioni rilevanti che consentono di gestire una connessione di rete sicura, usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.

Scopi del modulo

Chi supera la prova d'esame per questo modulo è in grado di:

- 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 d'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.
- 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.

1. Concetti di sicurezza

1.1. Minacce ai dati

1.1.1. Distinguere tra dati e informazioni.

1.1.2. Comprendere i termini "crimine informatico" e "hacking".

1.1.3. Riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne.

1.1.4. Riconoscere le minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti.

1.1.5. Riconoscere le minacce ai dati provocate dall'uso del cloud computing, quali: controllo sui dati, potenziale perdita di riservatezza (privacy).

1.2. Valore delle informazioni

1.2.1. Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali: confidenzialità, integrità, disponibilità.

1.2.2. Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto d'identità o le frodi, mantenere la riservatezza.

1.2.3. Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi.

1.2.4. Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni.

1.2.5. Comprendere i termini "soggetti dei dati" e "controllori dei dati", e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza.

1.2.6. Comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT e come fare per ottenerle.

1.3. Sicurezza personale

1.3.1. Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali accesso non autorizzato a sistemi informatici, raccolta non autorizzata di informazioni, frodi.

1.3.2. Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing (spiare alle spalle), al fine di carpire informazioni personali.

1.3.3. Comprendere il termine "furto di identità" e le sue implicazioni personali, finanziarie, lavorative, legali.

1.3.4. Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving); uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting).

1.4. Sicurezza dei file

1.4.1. Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro.

1.4.2. Comprendere i vantaggi e i limiti della cifratura. Comprendere l'importanza di non divulgare o di non perdere la password, la chiave o il certificato di cifratura.

1.4.3. Cifrare un file, una cartella, una unità disco.

1.4.4. Impostare una password per file quali: documenti, fogli di calcolo, file compressi.

2. Malware

2.1. Tipi e metodi

2.1.1. Comprendere il termine "malware". Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

2.1.2. Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm.

2.1.3. Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio: adware (proposta di pubblicità attraverso banner e popup), ransomware (blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo), spyware (software che invia ad un server remoto i dati di navigazione), botnet (software capace di prendere il controllo di una rete di computer), keylogger (software capace di inviare ad un server remoto i caratteri digitati su una tastiera) e dialer (software capace di cambiare la connessione del modem da un provider ad un altro).

2.2. Protezione
- 2.2.1. Comprendere come funziona il software antivirus e quali limitazioni presenta.
- 2.2.2. Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici.
- 2.2.3. Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.
- 2.2.4. Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus. Pianificare scansioni usando un software antivirus.
- 2.2.5. Comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.

2.3. Risoluzione e rimozione
- 2.3.1. Comprendere il termine "quarantena" e l'effetto di messa in quarantena file infetti/sospetti.
- 2.3.2. Mettere in quarantena, eliminare file infetti/sospetti.
- 2.3.3. Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte.

3. **Sicurezza in rete**

3.1. Reti e connessioni
- 3.1.1. Comprendere il termine "rete" e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WLAN (rete locale wireless), WAN (rete geografica), VPN (rete privata virtuale).
- 3.1.2. Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza.
- 3.1.3. Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete.
- 3.1.4. Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro.
- 3.1.5. Attivare, disattivare un firewall personale. Consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione.

3.2. Sicurezza su reti wireless
- 3.2.1. Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier).
- 3.2.2. Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (eavesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle).
- 3.2.3. Comprendere il termine "hotspot personale".
- 3.2.4. Attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici.

4. **Controllo di accesso**

4.1. Metodi
- 4.1.1. Identificare i metodi per impedire accessi non autorizzati ai dati, quali: nome utente, password, PIN, cifratura, autenticazione a più fattori.
- 4.1.2. Comprendere il termine "one-time password" e il suo utilizzo tipico.
- 4.1.3. Comprendere lo scopo di un account di rete.
- 4.1.4. Comprendere che per accedere alla rete sono necessari un nome utente e una password, e che è importante disconnettere l'account, al termine del collegamento.
- 4.1.5. Identificare le comuni tecniche di sicurezza biometrica usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano.

4.2. Gestione delle password
- 4.2.1. Riconoscere buone linee di condotta per la password, quali scegliere le password di lunghezza adeguata e contenenti un numero sufficiente di lettere, numeri e caratteri speciali; evitare di condividerle, modificarle con regolarità, scegliere password diverse per servizi diversi.
- 4.2.2. Comprendere la funzione e le limitazioni dei software di gestione delle password.

5. Uso sicuro del web

5.1. Impostazioni del browser
- 5.1.1. Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.
- 5.1.2. Eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di internet, password, cookie, dati per il completamento automatico.

5.2. Navigazione sicura in rete
- 5.2.1. Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura.
- 5.2.2. Identificare le modalità con cui confermare la autenticità di un sito web, quali: qualità del contenuto, attualità, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio.
- 5.2.3. Comprendere il termine "pharming".
- 5.2.4. Comprendere la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.

6. **Comunicazioni**

6.1. Posta elettronica
- 6.1.1. Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica.
- 6.1.2. Comprendere il termine "firma digitale".
- 6.1.3. Identificare i possibili messaggi fraudolenti o indesiderati.
- 6.1.4. Identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali.
- 6.1.5. Essere consapevoli che è possibile denunciare tentativi di phishing alle organizzazioni competenti o alle autorità

preposte.

6.1.6. Essere consapevoli del rischio di infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.

6.2. Reti sociali

6.2.1. Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.

6.2.2. Essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale, quali riservatezza dell'account e propria posizione.

6.2.3. Applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione.

6.2.4. Comprendere i pericoli potenziali connessi all'uso di siti di reti sociali, quali cyber bullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli.

6.2.5. Essere consapevoli che è possibile denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte.

6.3. VoIP e messaggistica istantanea

6.3.1. Comprendere le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP), quali malware, accesso da backdoor, accesso a file, intercettazione (eavesdropping).

6.3.2. Riconoscere i metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP (Voice over IP), quali cifratura, non divulgazione di informazioni importanti, limitazione alla condivisione di file.

6.4. Dispositivi mobili

6.4.1. Comprendere le possibili implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti.

6.4.2. Comprendere il termine "autorizzazioni dell'applicazione".

6.4.3. Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini.

6.4.4. Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo

7. Gestione sicura dei dati

7.1. Messa in sicurezza e salvataggio di dati

7.1.1. Riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, quali non lasciarli incustoditi, registrare la collocazione e i dettagli degli apparati, usare cavi antifurto, controllare gli accessi alle sale dei computer.

7.1.2. Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati da computer e da dispositivi mobili.

7.1.3. Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione del supporto dei dati salvati, compressione dei dati.

7.1.4. Effettuare la copia di sicurezza di dati su un supporto quale: unità disco/dispositivo locale, unità esterna, servizio su cloud.

7.1.5. Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud.

7.2. Cancellazione e distruzione sicura

7.2.1. Distinguere tra cancellare i dati ed eliminarli in modo permanente.

7.2.2. Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili.

7.2.3. Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente, come nel caso dei siti di reti sociali, blog, forum su internet, servizi su cloud.

7.2.4. Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di software per la cancellazione definitiva dei dati.

IT SECURITY

1 Concetti di sicurezza

1.1 MINACCE AI DATI

1.1.1 Distinguere tra dati e informazioni.

I **dati** sono numeri o altro (immagini, testo, ecc...) che rappresentano fatti o eventi non ancora organizzati. Le **informazioni** sono dati organizzati in modo da essere comprensibili e significativi per l'utente.

1.1.2 Comprendere il termine crimine informatico e "hacking".

Un **crimine informatico** è un crimine attuato per mezzo dell'abuso degli strumenti informatici, come computer e internet. Esempi di crimine informatico sono la frode informatica, il furto d'identità o l'accesso non autorizzato a sistemi informatici.

Per **hacking** si intende l'insieme dei metodi, delle tecniche e delle operazioni volte a conoscere, accedere e modificare un sistema informatico hardware o software. Questo termine ha assunto spesso una connotazione negativa in quanto associato a pratiche illecite, anche se a volte lo scopo dell'hacker è lecito, e consiste nel testare i sistemi informatici per verificarne l'affidabilità e la sicurezza.

1.1.3 Riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne.

In vari casi l'origine della perdita di dati può dipendere anche da fattori, dolosi o accidentali, come gli stessi **dipendenti di un'azienda** che, essendo autorizzati all'accesso ai dati, possono involontariamente perderli o anche rubarli per poi rivenderli.

Anche i **fornitori di servizi**, per esempio chi si occupa della manutenzione delle attrezzature hardware o dell'infrastruttura di rete, o dell'hosting del sito web aziendale potenzialmente sono in grado di danneggiare involontariamente i dati oppure di prenderne illegalmente possesso.

Infine può capitare che persone esterne, clienti e fornitori o semplici ospiti, possano accedere alla rete aziendale o scolastica tramite computer o altri dispositivi portatili, ad esempio tramite il Wi-Fi, e mettere a rischio i dati.

1.1.4 Riconoscere le minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti.

I **dati possono essere minacciati anche da eventi naturali** come incendi, inondazioni, terremoti. È pertanto necessario tenerne conto per prevenirne la perdita.

1.1.5 Riconoscere le minacce ai dati provocate dall'uso del cloud computing, quali: controllo sui dati, potenziale perdita di riservatezza (privacy).

Il cloud computing utilizza Internet per caricare dati su server remoti e per la collaborazione online tra membri della stessa organizzazione aziendale o scolastica. Ciò può portare, nel caso non sia stata implementata una corretta politica di accesso ai file e agli strumenti di comunicazione, a **rischi sul controllo dei dati** con potenziali ricadute sulla **privacy degli utenti e dei contenuti**.

1.2 VALORE DELLE INFORMAZIONI

1.2.1 Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali: confidenzialità, integrità, disponibilità.

Le caratteristiche fondamentali della sicurezza delle informazioni sono:

a) per **confidenzialità** si intende la riservatezza (privacy) dei dati contenuti, che devono poter essere utilizzati esclusivamente dal soggetto e dai titolari autorizzati al trattamento
b) per **integrità** si intende che le informazioni devono essere identiche all'originale, senza alcuna modifica o perdita di dati
c) per **disponibilità** si intende che le informazioni devono poter essere utilizzate in qualsiasi momento: anche a seguito di eventi naturali che possano aver distrutto gli originali deve essere disponibile una copia di backup identica all'originale.

1.2.2 Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto d'identità o le frodi, mantenere la riservatezza.

Le informazioni personali devono essere protette prima di tutto perché lo impone la legislazione europea (GDPR) e italiana (D.L. 10 agosto 2018, n. 101, che lo recepisce).

Inoltre è necessario proteggere le informazioni personali per evitare:

a) **furto d'identità**, attraverso il quale un malintenzionato potrebbe spacciarsi per qualcun altro e rubare informazioni personali o aziendali
b) **frodi** nei confronti della vittima del furto d'identità attraverso prelievi di denaro o spese non autorizzate o di terzi, attraverso l'utilizzo di credenziali riservate agli appartenenti a un'organizzazione
c) **perdita di riservatezza** di dati personali (indirizzo, numero di telefono, email, ecc…) o sensibili legati allo stato di salute, alle convinzioni religiose o politiche.

1.2.3 Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi.

Le **informazioni di carattere aziendale** trattano dati di clienti e informazioni di carattere finanziario, devono essere protette per evitare:

a) furti da parte di malintenzionati che potrebbero utilizzarle per fare concorrenza sleale
b) utilizzi fraudolenti, per esempio legati allo spionaggio industriale
c) perdite accidentali di dati, che renderebbero difficile una gestione corretta e aderente alla normativa vigente
d) sabotaggi da parte di malintenzionati.

Nel caso avvenissero perdite di dati, i controllori del trattamento ne sarebbero responsabili di fronte all'azienda e pertanto perseguibili.

1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni.

Chi gestisce dati e informazioni deve rifarsi alla normativa vigente che, in Italia, che si è evoluta nel corso del tempo e che fa riferimento al D.L. n. 5 del 9 febbraio 2012 che ha preso il posto del precedente D.L. 196/2003. Nel 2016 è stato approvato dall'UE il GDPR (General Data Protection Regulament) entrato in vigore il 25 maggio 2018 e recepito dal D.L. 101 del 10 agosto 2018.

Questa normativa mette in luce i seguenti principi comuni relativamente alla protezione, conservazione e controllo dei dati e della riservatezza:

a) **trasparenza**, il soggetto delle informazioni deve essere al corrente che i suoi dati sono trattati da terze persone (art.5 comma a del GDPR)
b) gli **scopi del trattamento devono essere legittimi**, per esempio perché autorizzati dal soggetto o perché necessari agli scopi istituzionali di chi li trattamenti (art.5 comma b e art.6 del GDPR)
c) le **misure di protezione dei dati devono essere proporzionali rispetto a eventuali danni**, pertanto è opportuno che venga svolta un'analisi del rischio: eventi gravi ma remoti o eventi probabili ma di scarsissima entità permettono misure molto semplici, mentre danni significativi con possibilità concrete impongono misure di protezione appropriate, che in alcuni casi possono essere impegnative da un punto di vista organizzativo (possono richiedere l'intervento di un'azienda specializzata) ed economico.

1.2.5 Comprendere i termini "soggetti dei dati" e "controllori dei dati", e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza.

Il **soggetto dei dati** è la persona o l'azienda cui appartengono i dati e può dare il permesso a terzi di conoscere, utilizzare e conservare i propri dati per vari motivi:

a) perché necessari per svolgere un compito istituzionale o un servizio, ad esempio prenotare una visita medica, iscriversi a scuola o effettuare un bonifico bancario
b) a scopo di marketing da parte di aziende che li richiedono in cambio di servizi aggiuntivi gratuiti, ad esempio le tessere fedeltà dei supermercati, la possibilità di accedere ai media sociali, ecc...

Il **controllore dei dati** è la persona o l'azienda che conosce, utilizza e conserva i dati per motivi istituzionali o di marketing. Questo soggetto deve garantire al soggetto dei dati la trasparenza, la legittimità e la protezione dei dati stessi, ed è penalmente perseguibile se non lo fa.

1.2.6 Comprendere l’importanza di attenersi alle linee guida e alle politiche per l’uso dell’ICT e come fare per ottenerle.

È pertanto estremamente importante attenersi alla normativa che disciplina l'utilizzo delle tecnologie informatiche e delle telecomunicazioni (ICT) per preservare i dati, personali e aziendali, dal furto, dallo smarrimento e da un utilizzo non consentito.

Ciascun settore lavorativo o azienda dispone di uno o più responsabili per la sicurezza informatica e proprie linee guida specifiche". Occorre informarsi per sapere a chi chiedere in azienda le linee guida che si applicano in quella realtà. In linea di massima questa figura è, a seguito dell’adozione del GDPR, il DPO (Data Protection Officer, responsabile per la protezione dei dati) che le aziende e gli enti sono obbligate ad avere tra il personale interno o dando l’incarico a un professionista esterno.

1.3 SICUREZZA PERSONALE

1.3.1 Comprendere il termine “ingegneria sociale” e le sue implicazioni, quali accesso non autorizzato a sistemi informatici, raccolta non autorizzata d'informazioni, frodi.

L'**ingegneria sociale** (dall'inglese social engineering) è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili manipolando i soggetti affinché attuino comportamenti che mettono a rischio la sicurezza dei propri dati e informazioni.

Viene a volte utilizzata, al posto delle tecniche di hacking, per accedere a informazioni riservate aggirando sistemi di protezione hardware e software dei dati sempre più sofisticati e difficilmente penetrabili.

1.3.2 Identificare i metodi applicati dall’ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing al fine di carpire informazioni personali.

Uno dei metodi utilizzati sono le **chiamate telefoniche** che, a volte promettendo premi, cercano di ottenere informazioni personali mascherandole con sondaggi anonimi.

Il **phishing** (dal verbo inglese to fish, pescare) è una tecnica basata sull'invio d'ingannevoli messaggi di posta elettronica: il phisher si finge un servizio bancario e, minacciando la chiusura del conto o della carta di credito, chiede d'inserire le proprie credenziali per poterle verificare. Ovviamente si tratta di un trucco per entrarne in possesso.

Il **shoulder surfing** (fare surf sulla spalla) consiste nel carpire le credenziali immesse dall'utente di un servizio spiandolo direttamente, standogli nei pressi, oppure anche da lontano, per mezzo di lenti o telecamere. Ciò può avvenire generalmente in luoghi affollati, come internet cafè o simili.

1.3.3 Comprendere il termine furto d'identità e le sue implicazioni personali, finanziarie, lavorative, legali.

Il **furto d'identità** nel campo informatico consiste nell'appropriazione indebita delle credenziali di accesso a un servizio (accesso a un PC, a una rete locale, a internet, alla posta elettronica, a una rete sociale, a un servizio d'internet banking) allo scopo di usarlo a proprio vantaggio, per compiere crimini informatici con varie implicazioni negative per la persona derubata:

a) **personali**, quando il furto d’identità riguarda per esempio account di reti sociali che possono essere usate a sproposito
b) **finanziarie**, se il furto riguarda account di home banking o numeri di carte di credito, che possono essere utilizzate per operazioni finanziarie a danno del derubato (furti, utilizzi indebiti, ecc...)
c) **lavorative**, nel caso in cui riguardi account utilizzati nell’attività lavorativa possono portare a furti di dati riservati di proprietà aziendale, con negative conseguenze per l’azienda che potrebbe rivalersi sul dipendente la cui identità digitale è stata rubata
d) **legali**, nel caso l’identità digitale venga utilizzata per compiere crimini informatici, il derubato può essere accusato di non aver custodito in modo adeguato o di non aver tempestivamente denunciato il furto d’identità.

1.3.4 Identificare i metodi applicati per il furto d'identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving); uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting).

Per attuare il furto d'identità vengono usati vari metodi, tra cui:

a) l’**information diving** che consiste nel frugare negli scarti delle persone tra cui potrebbe nascondersi

qualche riferimento ai propri dati sensibili che possono essere stati memorizzati in un dispositivo dismesso o anche fogli di appunti cartacei. Per evitare ciò è importante cancellare in modo sicuro la memoria di computer, smartphone e tablet prima di eliminarli

b) lo **skimming**, che consiste nell'acquisire dati della carta di credito o di debito quando si preleva contante da un bancomat o si striscia la carta in un esercizio commerciale. In certi casi ciò è associato allo shoulder surfing attraverso il quale si spia l'utente quando inserisce il PIN. Questo modo di rubare l'identità negli ultimi tempi è diventato più difficile con la diffusione delle carte contactless

c) il **pretexting** è una forma d'ingegneria sociale che si prefigge di carpire informazioni personali simulando, generalmente attraverso il telefono, uno scenario (richiesta d'informazioni da parte dell'autorità) che mette in soggezione la vittima e la induce a fornire dati riservati.

1.4 SICUREZZA DEI FILE

1.4.1 Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza relative alle macro.

Una macro è un insieme d'istruzioni, a volte molto complesse e che utilizzano un linguaggio di programmazione (come Visual Basic o LibreOffice Basic) che possono essere eseguite, all'interno di un software di produttività (videoscrittura, foglio di calcolo, ecc...) automaticamente o alla pressione di una combinazione di tasti.

Le macro sono strumenti molto utili perché automatizzano procedure lunghe e noiose, ma possono contenere codice malevolo che quindi può causare danni al computer. Ciò vale soprattutto quando l'origine della macro non è certa.

Pertanto **attivare una macro** ne consente l'esecuzione con i vantaggi sopra descritti, ma può mettere a rischio il computer.

Al contrario, **disattivare una macro** non ne consente l'esecuzione e quindi impedisce di avvalersi delle sue funzionalità, ma mette al sicuro il computer da possibile codice malevolo.

In linea di massima la cosa migliore è attivare le macro di cui si è certi, e disattivare quelle d'incerta provenienza.

1.4.2 Comprendere i vantaggi e i limiti della cifratura. Comprendere l'importanza di non divulgare o di non perdere la password, la chiave o il certificato di cifratura.

Cifrare un file consiste nell'utilizzare un algoritmo crittografico per renderlo illeggibile senza la relativa chiave di decifrazione, che può consistere in una password, una chiave o un certificato digitale.

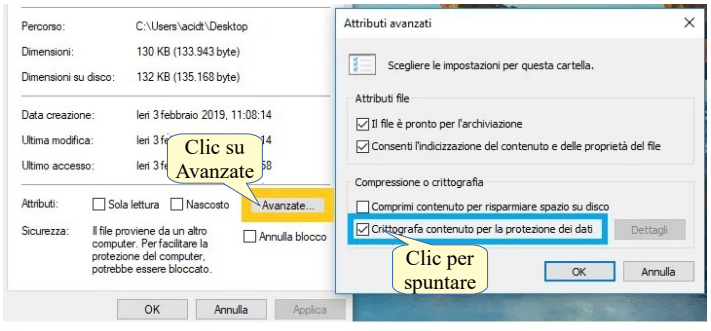
Ciò garantisce che i dati in esso contenuti siano confidenziali e non cadano nelle mani sbagliate. È importante che la chiave di decifrazione:

a) **non venga persa**, altrimenti non sarà più possibile utilizzare il contenuto del file cifrato
b) **non venga divulgata**, altrimenti altre persone potranno accedere al contenuto del file.

1.4.3 Cifrare un file, una cartella, una unità disco.

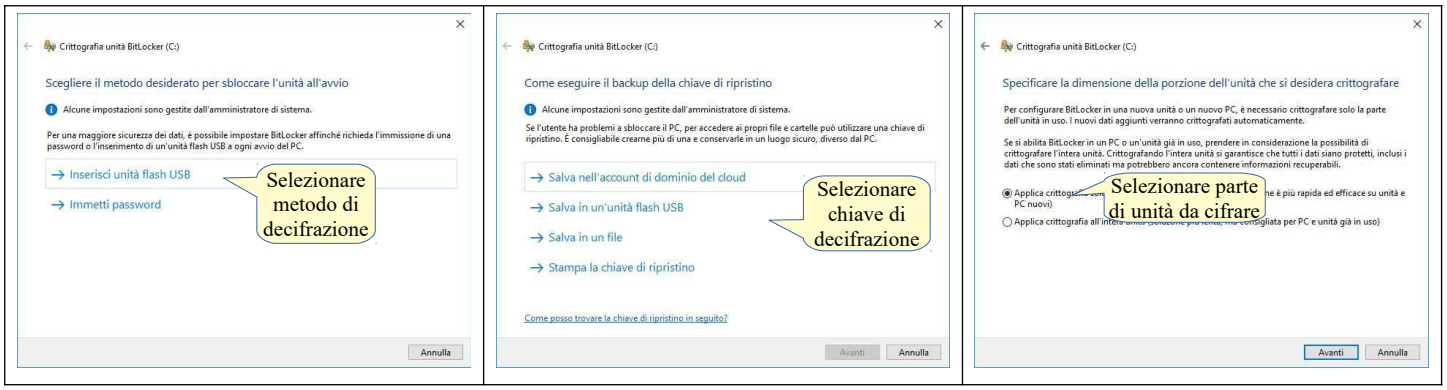
Per **cifrare un file, una cartella**, con Windows 10 Professional (la versione Home non dispone di questa funzionalità) occorre cliccare col pulsante destro del mouse sul file o la cartella da cifrare, e scegliere Proprietà nel menu contestuale cui si accede, poi cliccare sulla scheda Avanzate e spuntare la casella di controllo Crittografa contenuto per la protezione dei dati. Con altre versioni di Windows o con Ubuntu per cifrare file e cartelle occorre utilizzare software specifici.

FinalCrypt in ambiente Ubuntu



Cifratura in Windows 10 Professional

Per **cifrare un'unità disco** con Windows 10 Professional (Windows 10 Home non dispone di questa utilità) si può utilizzare Bitlocker. Con altri siatemi operativi occorre utilizzare un software specifico come per esempio Veracrypt, un software libero e disponibile per tutti i sistemi operativi.

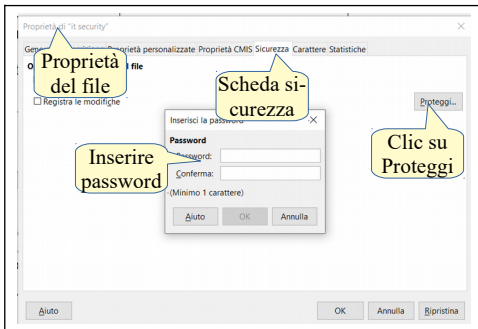


1.4.4 Impostare una password per file quali documenti, file compressi, fogli di calcolo.

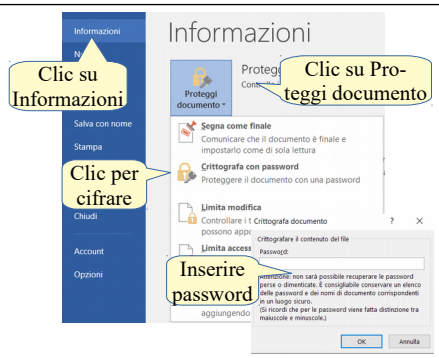
Per **impostare una password di accesso ai file** è possibile utilizzare le funzioni presenti in molti programmi di produttività o di utilità, come i software di compressione di file e cartelle. Per farlo utilizzando una qualsiasi delle applicazioni di LibreOffice (Writer, Calc, Impress, ecc…) occorre:

a) aprire il file da proteggere
b) scegliere Proprietà... dal menu File
c) nella scheda Sicurezza cliccare sul pulsante Proteggi...
d) inserire e confermare la password da applicare.

Per proteggere un documento Word o Excel occorre cliccare su File > Informazioni, poi cliccare sull'icona Proteggi documento / Proteggi cartella di lavoro e selezionare Crittografa con password. Infine inserire una password, che non necessita di essere confermata.



Proteggere un documento o foglio di calcolo LibreOffice

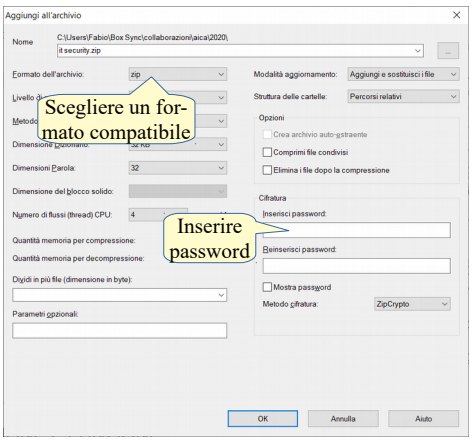


Proteggere un documento Word

Proteggere una cartella di lavoro Excel

Per **proteggere con password un archivio compresso**, in ambiente Windows occorre utilizzare un software specifico, per esempio il software libero 7zip esistente anche per sistema operativo Linux, dato che l'utilità del sistema operativo permette di creare archivi compressi, ma non di proteggerli con password. Con 7zip occorre durante la creazione di un archivio compresso inserire e confermare una password (da notare che ciò è possibile solo con alcuni formati di compressione, tra cui 7z e zip). Non è possibile proteggere un archivio già creato in precedenza.

In ambiente Ubuntu 18.04 è possibile creare e proteggere archivi compressi senza installare software specifici, utilizzando solo le funzioni dell'utilità di gestione dei File. Per farlo occorre prima di tutto creare l'archivio compresso scegliendo dal menu contestuale la voce Comprimi...



Creare e proteggere un archivio compresso con 7zip

Creare un archivio compresso in ambiente Ubuntu 18.04

Proteggere un archivio compresso in ambiente Ubuntu 18.04

2 Malware

2.1 TIPI E METODI

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Il termine **malware indica un software creato con lo scopo di causare danni** più o meno gravi a un sistema informatico su cui viene eseguito e ai dati degli utenti, generalmente allo scopo di trarne vantaggio.

Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malevolo".

I malware sono realizzati in modo da mimetizzarsi all’interno dei sistemi informatici:

a) per **Trojan horse** (cavallo di Troia) si intende un software che, oltre ad avere delle funzionalità "lecite", utili per indurre l'utente a utilizzarlo, contiene istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore
b) per **Backdoor** (porta sul retro) si intende un software che consente un accesso non autorizzato al sistema sul quale è in esecuzione
c) per **Rootkit** si intende un software ben nascosto nei meandri del sistema operativo che permette a malintenzionati d'installare nel computer strumenti di controllo remoto.

2.1.2 Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm.

Alcuni malware hanno lo scopo d'infettare i sistemi informatici:

a) i **Virus** sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti a opera degli utenti (siti web, messaggi di posta elettronica, utilizzo di unità di memoria portatili, ecc...)
b) i **Worm** non hanno bisogno d'infettare altri file per diffondersi, perché modificano il sistema operativo in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti a eseguirli utilizzano tecniche d'ingegneria sociale, oppure sfruttano dei difetti (bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

2.1.3 Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio: adware (proposta di pubblicità attraverso banner e popup), ransomware (blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo), spyware (software che invia a un server remoto i dati di navigazione), botnet (software capace di prendere il controllo di una rete di computer), keylogger (software capace di inviare ad un server remoto i caratteri digitati su una tastiera) e dialer (software capace di cambiare la connessione del modem da un provider ad un altro).

Alcuni malware hanno lo scopo di carpire dati o di ottenere profitto economico anche attraverso l’estorsione:

a) gli **adware** sono software che presentano all'utente messaggi pubblicitari durante l'uso, generalmente in finestre popup che si aprono automaticamente durante la navigazione su Internet tramite un browser. Possono causare danni quali rallentamenti del PC e rischi per la privacy in quanto comunicano le abitudini di navigazione a server remoti
b) i **ransomware** sono dei software che bloccano l'accesso ai sistemi o ai file personali degli utenti e chiedono il pagamento di un riscatto per renderli nuovamente accessibili. Si diffondono spesso attraverso messaggi di spam e tecniche di ingegneria sociale che inducono i destinatari ad aprire gli allegati o a cliccare su link che portano a siti web apparentemente legittimi
c) gli **spyware** sono software che hanno lo scopo raccogliere informazioni (memorizzazione di tasti premuti, screenshot, credenziali di autenticazione, indirizzi e-mail personali, dati ricavati da moduli web, informazioni sull'uso d'internet e altri dati personali, come i numeri di carta di credito) per trasmetterle a malintenzionati
d) una **botnet** è una rete di computer infettati da un malware che li mette in comunicazione tra di loro e col botmaster, che la controlla da remoto. Lo scopo è utilizzare la rete stessa e i dispositivi a essa collegati per svolgere attività non autorizzate, come l'invio di spam, rubare i dati personali o lanciare attacchi DDoS (Distributed Denial of Service) che si propongono d'impedire l'uso di una risorsa di rete, ad esempio un sito web, attraverso massicce richieste al server che fornisce il servizio fino a bloccarlo
e) i **keylogger** sono software in grado di registrare tutto ciò che viene digitato sulla tastiera consentendo il furto di dati personali, come le credenziali di accesso, il numero della carta di credito, ecc...
f) I **dialer** sono software che modificano, quando ci si connette con la normale linea telefonica, il numero chiamato dalla connessione predefinita con uno a tariffazione speciale allo scopo di trarne illecito profitto all'insaputa dell'utente. Questo tipo di malware oggi non è più diffuso in quanto le connessioni a internet sono ormai tutte digitali (ADSL, fibra, ecc…).

2.2 PROTEZIONE

2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta.

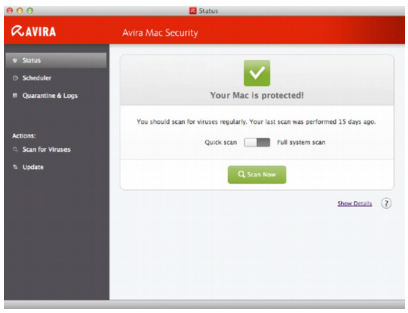
Soprattutto sui dispositivi con sistema operativo Windows, è necessario avere installato un software antivirus, che sia in grado di opporsi ai tentativi dei malware d'infettare il sistema. In realtà nessun sistema operativo è immune dai malware, ma Windows è più vulnerabile sia per motivi strutturali, sia per il fatto che, essendo più diffuso degli altri, viene maggiormente preso di mira da questi software.

Un **antivirus ha due funzioni principali**:
a) la prima è di controllare cartelle e file in modo da individuare e rendere innocui eventuali file portatori d'infezione virale
b) la seconda è scansionare in tempo reale la memoria RAM in modo da impedire l'esecuzione di codice virale, che è in grado di riconoscere per un confronto con un archivio contenente le "firme" dei malware conosciuti, o anche con metodi d'indagine euristica, cioè basata sulla somiglianza di frammenti di codice virale con quello analizzato.

Un **antivirus non può essere efficace al 100%** e proteggere completamente un dispositivo informatico:
a) alcuni malware possono sfuggire al controllo di un antivirus ed essere individuati da un altro
b) per poter essere efficace, l'antivirus deve essere aggiornato con frequenza, in particolare l'archivio delle firme, in quanto nuovi malware vengono diffusi in continuazione
c) un altro limite che i software antivirus hanno, è che a volte segnalano falsi positivi, cioè indicano come virus programmi del tutto leciti.

L'antivirus integrato in Windows 10

Clamtk, antivirus per Linux



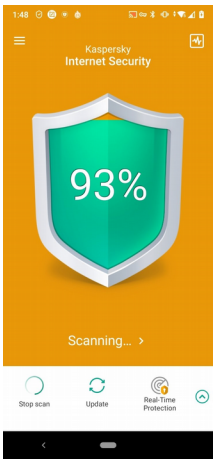
Un antivirus per Mac OSX

2.2.2 Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici.

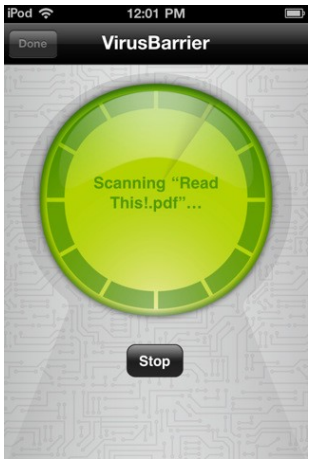
Anche se il sistema operativo Windows è più vulnerabile di altri ai malware, è opportuno avere software antivirus su qualsiasi dispositivo informatico:

a) computer con sistema operativo Windows, Mac OSX, Linux
b) dispositivi mobili con sistema operativo Android o iOS
c) server, che devono ospitare grandi quantità di file e servizi che coinvolgono numerosi utenti (siti web, email, ecc...).

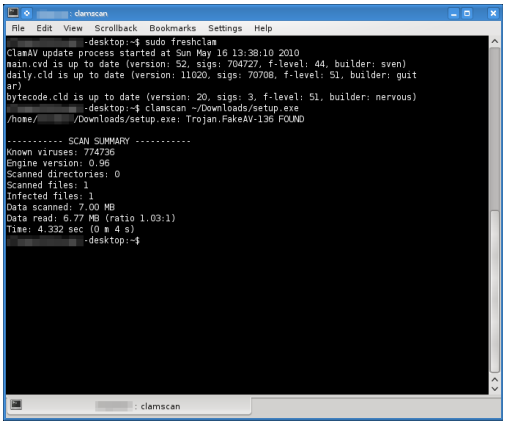
Ciascuno di questi dispositivi necessità di software antivirus dedicati, con prestazioni e modalità di analisi differenti in base all'hardware, al sistema operativo utilizzato e all'utilizzo che ne viene fatto.



Un antivirus per Android



Un antivirus per iOS



Clam, antivirus a linea di comando per server Linux e Unix

2.2.3 Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.

Qualsiasi software contiene dei bug, cioè degli errori e delle vulnerabilità, che possono essere sfruttati da malintenzionati per attacchi informatici. Chi produce i software pertanto monitora gli utenti e ha tra i propri dipendenti degli esperti hacker (vedi punto 1.1.2) per verificare l'esistenza di bug e per sviluppare soluzioni, che vengono distribuite agli utenti tramite gli aggiornamenti. Una cosa per certi aspetti simile avviene con le campagne di richiamo per prodotti materiali che, al contrario dei software, devono essere portati fisicamente nei centri di riparazione.

In particolare **è necessario aggiornare**:

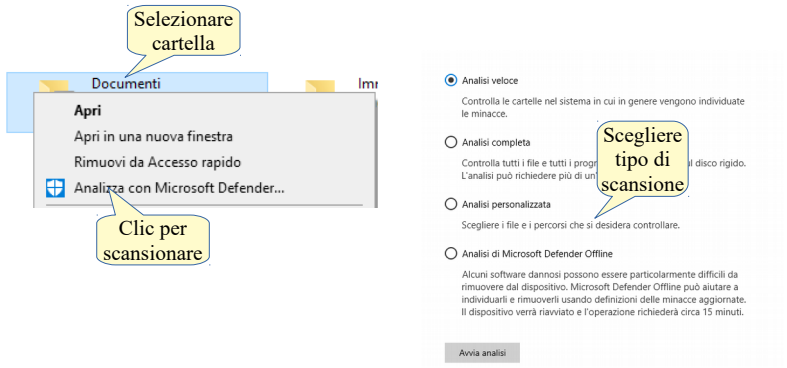
a) gli **antivirus** sono i software che devono essere aggiornati più di frequente in quanto la loro azione si basa sul riconoscimento del codice dei malware, che vengono sviluppati in continuazione. L'aggiornamento delle definizioni dei virus devono essere aggiornate molto spesso, anche più di una volta al giorno, pertanto questi software generalmente svolgono questi aggiornamenti in modo automatico
b) i **browser web** sono software molto utilizzati per accedere a siti web che possono contenere software malevolo in grado di sfruttarne le vulnerabilità. Anche questi software vengono aggiornati frequentemente e in modalità automatica
c) i **client di posta elettronica** che vengono utilizzati per inviare, scaricare leggere messaggi che spesso sono veicoli di diffusione di malware, vengono aggiornati di frequentemente
d) i **plug-in**, in particolare quelli dei browser, devono essere aggiornati con frequenza perché spesso le loro vulnerabilità sono sfruttate dai malware
e) le **applicazioni** con cui apriamo e modifichiamo documenti di testo, fogli di calcolo, presentazioni, ecc… vanno aggiornate perché i loro bug possono essere sfruttati da software malevolo
f) il **sistema operativo** che è il software di gran lunga più complesso e articolato, può avere moltissime vulnerabilità e pertanto deve essere aggiornato per evitare che queste possano essere sfruttate da malware.

2.2.4 Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus. Pianificare scansioni usando un software antivirus.

In ambiente Windows tutti i software antivirus permettono la scansione di file e cartelle. Per **eseguire una scansione** con l'antivirus integrato del sistema operativo Windows Defender occorre cliccare col pulsante

destro del mouse sul file o cartella da analizzare e scegliere Analizza con Microsoft Defender nel menu contestuale. Nella finestra cui si accede si può selezionare il tipo di scansione, ma non è possibile pianificare scansioni. Con altri software antivirus anche gratuiti (nell'esempio Avira free) è possibile non solo effettuare una scansione istantanea, ma anche pianificare scansioni giornaliere, settimanali o mensili.

Per **pianificare una scansione** occorre avviare l'interfaccia del software, accedere all'area scansioni e impostare una scansione personalizzata, assegnandole un nome, selezionando la cartella da analizzare e scegliendo una frequenza (giornaliera, settimanale, mensili).



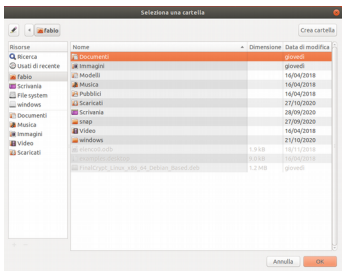
Avviare una scansione con Windows Defender

Pianificare una scansione con Avira

In ambiente Linux esistono pochi software antivirus dei quali il solo ClamAv, un antivirus utilizzato generalmente sui server da linea di comando, è open source. Esiste un'interfaccia grafica denominata ClamTK, che si può installare utilizzando Ubuntu Software o da terminale col comando sudo apt install clamtk.

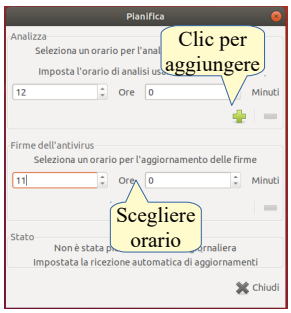
Per **eseguire la scansione** di un file o di una cartella con ClamTK in ambiente Linux occorre cliccare sull'icona Analizza un file o Analizza una cartella e, nella finestra cui si accede, selezionare il file o la cartella. Per **pianificare una scansione** (possibile solo la scansione giornaliera) occorre cliccare sull'icona Pianificatore e impostare l'orario; fatto ciò occorre cliccare sull'icona Aggiungi.

ClamTK



Scelta della cartella

Risultati analisi



Pianificazione

2.2.5 Comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.

Software obsoleto e non più supportato da parte del produttore può portare dei rischi in quanto:

a) la **mancanza di aggiornamenti rende possibile al malware sfruttare bug e vulnerabilità** per furti d'identità o altre forme di attacco
b) **software obsoleto potrebbe non essere compatibile** con un sistema operativo o con un hardware aggiornato che non permette l'utilizzo di periferiche datate ma necessarie per il software in questione (es. porte di input/output legacy).

2.3 RISOLUZIONE E RIMOZIONE

2.3.1 Comprendere il termine quarantena e l'operazione di mettere in quarantena file infetti/sospetti.

Per **Quarantena si intende lo spostamento dei file infetti o sospetti in una posizione sicura** del file system e nel **renderli non eseguibili**.

Quando un software antivirus individua dei file contenenti del codice virale o anche solo sospetti, avvisa l'utente che intende spostarli in un'apposita cartella creata dal software antivirus e pertanto facilmente controllabile, e resi non eseguibili attraverso la modifica dei permessi (in ambiente Linux o Mac) o

dell'estensione del file (in ambiente Windows).

2.3.2 Mettere in quarantena, eliminare file infetti/sospetti.

Generalmente i **software antivirus spostano automaticamente i file infetti o sospetti in quarantena**, mentre alcuni chiedono conferma all'utente, che deve solo confermare lo spostamento, a meno che sia certo che si tratti di un falso positivo.

I software antivirus danno la possibilità di visualizzare i file infetti o sospetti spostati in quarantena, e di eliminarli o ripristinarli, nel caso si sia certi che si tratta di un falso positivo.

Quarantena in Avira per Windows

Quarantena in ClamTK

2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte.

I produttori di software mettono a disposizione **risorse online per diagnosticare e risolvere attacchi di malware** e, in particolare:

a) i produttori di **sistemi operativi** sono particolarmente attenti a fornire tutte le istruzioni per aiutare i propri utenti a ridurre i rischi provocati dal malware

Sito web di Microsoft con istruzioni sul malware

Sito web di Apple con istruzioni sul malware

b) alcuni produttori di **antivirus** mettono a disposizione, oltre al supporto, anche strumenti di scansione e rimozione online

c) i produttori di **browser web** segnalano se sono installate estensioni non sicure, per esempio Adobe Flash, e invitano a disabilitarlo

d) i siti web delle **autorità preposte** segnalano minacce legate al malware.

Sito web che permette la scansione online

Sito web dell'AGID con informazioni sui pericoli del malware

3 Sicurezza in rete

3.1 RETI

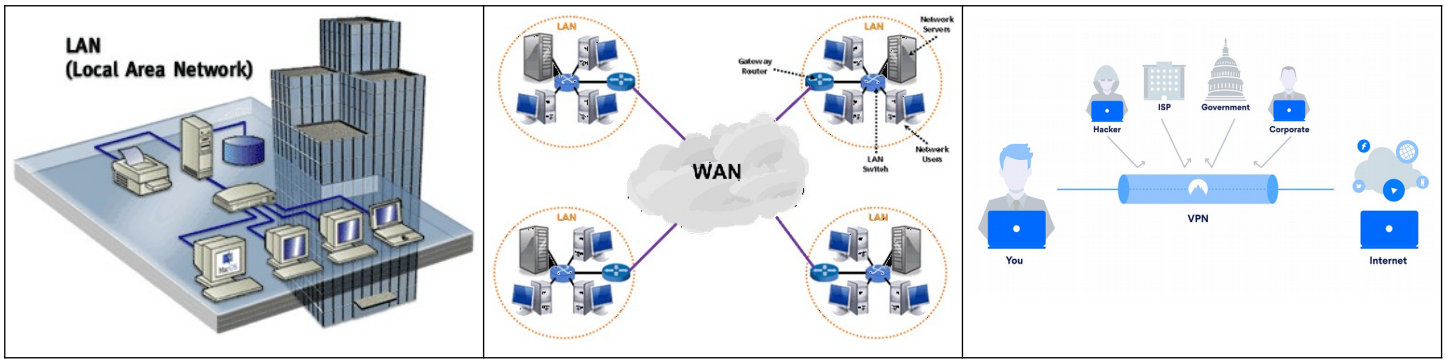
3.1.1 Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale).

Una rete informatica comprende più dispositivi, come server, personal computer, dispositivi mobili, apparati di rete, in grado di comunicare tra di essi in vari modi, cablati o senza fili (wireless).

Una rete può essere limitata nello spazio, per esempio a un locale o a un edificio e prende il nome di **LAN** (Local Area Network).

Se la rete è estesa a un'area cittadina prende il nome di **MAN** (Metropolitan Area Network). Se la rete è molto estesa come ad esempio Internet, prende il nome di **WAN** (Wide Area Network).

Una **VPN** (Virtual Private Network) è un sistema per far transitare dati in modo privato attraverso una rete pubblica. Normalmente una VPN viene implementata per poter collegare in modo sicuro più computer lontani tra di loro attraverso Internet. Un apposito software si occupa di creare un tunnel sicuro attraverso la cifratura dei dati e l'autenticazione della comunicazione (vedi punto 1.4.2).



3.1.2 Comprendere che la connessione a una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza.

Un computer trae grandi vantaggi dalla connessione a una rete, e tuttavia dalla rete possono arrivare anche minacce.

Attraverso la rete, locale o internet, **è possibile che il computer venga infettato da virus o altro malware** che spesso viene scaricato da internet attraverso la posta elettronica o pagine web.

Attraverso la rete **sono possibili accessi non autorizzati ai dispositivi connessi**, dovuti a falle di sicurezza o infezioni virali.

La rete **può mettere a rischio anche la privacy** degli utenti connessi, in quanto i dati personali, se non adeguatamente protetti, possono essere accessibili da persone interessate in vari modi, come accennato in precedenza.

3.1.3 Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete.

Una rete viene gestita da un amministratore che si occupa di renderla sicura ed efficiente attraverso l'implementazione di diversi aspetti:

a) **modalità di autenticazione** degli utenti che accedono alla rete, che generalmente avviene attraverso l'**assegnazione di account**, formati da nome utente e relativa password, differenziati in base alle necessità dei singoli e dei gruppi di lavoro
b) sicurezza dei dispositivi connessi alla rete attraverso il controllo degli aggiornamenti software (vedi anche punto 2.2.3) e delle relative patch di sicurezza
c) **controllo del traffico di rete** attraverso dispositivi hardware come i firewall o appositi software che svolgono questo compito
d) **rilevazione delle minacce legate al malware** attraverso software antivirus e loro **rimozione**.

3.1.4 Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro.

Un **firewall è un dispositivo o un software che ha la funzione di monitorare e controllare il traffico di rete** tra il singolo dispositivo o la rete locale (LAN) e internet, allo scopo di evitare intrusioni e accessi non autorizzati in base a delle regole definite dall'amministratore.

I **limiti di un firewall** sono che:

a) per funzionare bene il firewall deve essere programmato in modo efficace, dato che si limita a seguire le regole impostate. Se le regole non sono ben organizzate il funzionamento del firewall non sarà efficace.
b) dato che il firewall è generalmente posto tra la rete locale e internet, non avrà effetto se l'attacco alla rete viene effettuato dall'interno, per esempio da un utente della rete o dal un malware che precedentemente ha infettato un dispositivo della rete.
c) un firewall, soprattutto se mal programmato, può impedire agli utenti un uso legittimo della rete.

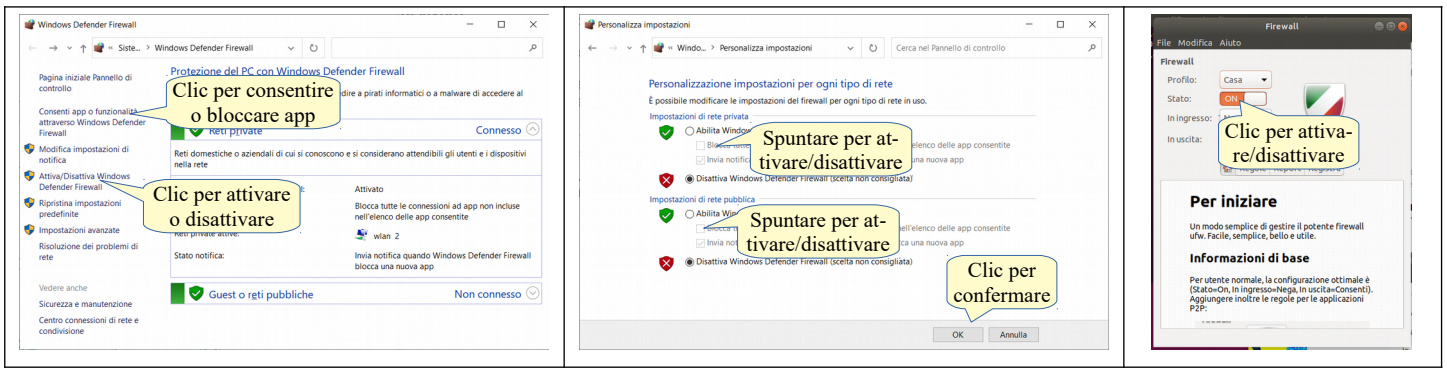
3.1.5 Attivare, disattivare un firewall personale. Consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione.

Un firewall personale è quasi sempre un software residente sul computer che normalmente non richiede alcun intervento da parte dell'utente, che tuttavia sono possibili in caso di necessità da parte di utenti competenti, dato che interventi errati possono pregiudicare la funzionalità e la sicurezza del dispositivo.

In **ambiente Windows 10** il firewall personale viene avviato in automatico dal sistema operativo all'accensione del computer. Nel caso sia spento, per attivare o disattivare Windows Defender firewall che prendiamo come esempio, occorre accedere alle impostazioni di Windows, avviare l'applet del firewall e cliccare su Attiva/Disattiva Windows Defender firewall. Nella finestra cui si accede occorre spuntare l'opzione desiderata per la rete privata e/o per la rete pubblica, infine cliccare su OK.

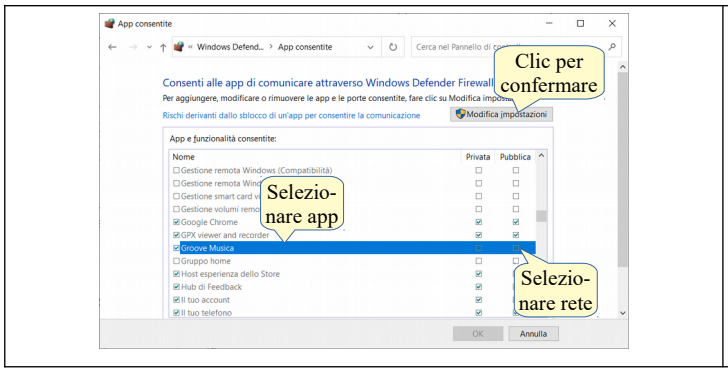
In **ambiente Ubuntu 18.04** il firewall personale di default è UFW (Uncomplicated FireWall) e la sua interfaccia grafica Gufw. Se non fossero già installati, lo si può fare utilizzando Ubuntu Software (vedi la dispensa Computer essentials, punto 2.3.6).

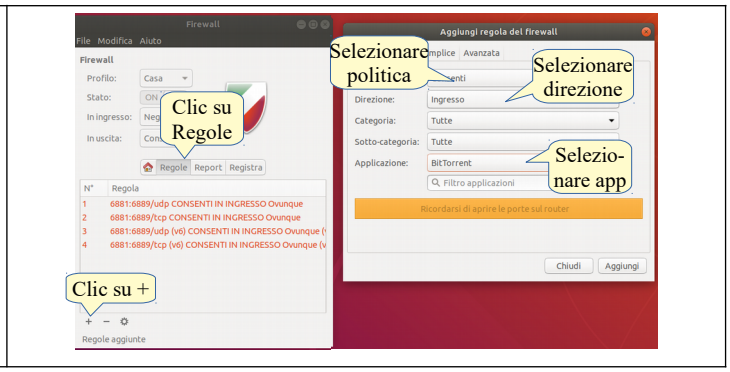
Per avviare il firewall occorre accedere a Mostra applicazioni, digitare gufw e selezionare l'icona dell'applicazione. Per **attivare o disattivare il firewall** nella finestra dell'applicazione cliccare sul pulsante Stato.



Per consentire o bloccare l'accesso a un'applicazione in ambiente Windows 10 con Windows Defender firewall occorre cliccare su Consenti app o funzionalità, selezionare l'app e cliccare su Modifica Impostazioni.

Per **consentire o bloccare l'accesso a un'applicazione** in **ambiente Ubuntu 18.04** con Gufw occorre cliccare su Regole e poi su +. Nella finestra cui si accede occorre selezionare l'applicazione cui consentire o bloccare l'accesso e impostare altri parametri (consenti/blocca, ingresso/uscita, ecc…). Infine cliccare su Aggiungi.





3.2 SICUREZZA SU RETI WIRELESS

3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier).

Per migliorare la sicurezza delle reti wireless nel corso degli anni sono stati elaborati degli algoritmi di cifratura dei dati trasmessi nelle reti senza fili:

a) il **WEP** (Wired Equivalent Privacy, cioè sicurezza della privacy equivalente a quella delle reti cablate) nasce nel 1999 ma nel giro di pochi anni si è verificato che non è adeguatamente sicuro, in quanto essendo la chiave troppo breve, è abbastanza facile individuarla e poter quindi accedere
b) il **WPA** (Wi-Fi Protected Access, accesso protetto alle reti senza fili) è stato elaborato nel 2003 e mette a disposizione una maggiore sicurezza rispetto al precedente WEP, che tuttavia non è totale
c) il **WPA2** (Wi-Fi Protected Access 2, accesso protetto alle reti senza fili, versione 2) è la versione aggiornata nel 2004 del WPA e offre maggiore sicurezza in quanto basato su una chiave AES più robusta. Questo protocollo nel 2006 è diventato obbligatorio per i dispositivi certificati Wi-Fi. Nel 2018 è stata resa disponibile la versione 3 di WPA
d) Il **filtraggio MAC** consiste nel permettere l'accesso a una rete Wi-Fi esclusivamente ai dispositivi che dispongono di una scheda di rete il cui indirizzo fisico (MAC, Media Access Control). Ciò consente di stilare all'interno degli apparati di rete delle ACL (Access List, liste di indirizzi MAC) di dispositivi autorizzati all'accesso alla rete. Un dispositivo con un Mac address differente, anche se il proprietario conosce la password di accesso alla rete senza fili, non verrà connesso alla rete. Anche questo metodo in realtà non è del tutto sicuro, in quanto esistono dei software in grado di modificare il Mac address della scheda di rete di un dispositivo
e) **nascondere l'SSID** (Service Set Identifier, il nome della rete Wi-Fi) rende più difficoltoso a terzi l'accesso a una rete perché deve conoscerne anche il nome oltre alle credenziali.

Come si può capire da quanto detto in precedenza, nessun metodo rende sicura al 100% una rete senza fili, tuttavia utilizzando più metodi in combinazione si raggiunge un buon grado di sicurezza.

3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (eavesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle).

Se una rete senza fili non è protetta con uno o più dei metodi sopra presentati, è molto facile che qualche malintenzionato possa accedervi e quindi abbia la possibilità d'intercettare i dati presenti sui dispositivi connessi o anche solo in transito. Ciò può avvenire in diversi modi:

a) l'**intercettazione** delle comunicazioni (eavesdropping) è un attacco informatico che permette di ascoltare di nascosto la conversazione privata o le comunicazioni di altri senza il loro consenso al fine di raccogliere informazioni
b) il **dirottamento di rete** (network hijacking) è un attacco informatico che reindirizza gli indirizzi IP (protocollo Internet) senza autorizzazione. Spesso questo attacco fa sì che l'utente acceda a contenuti diversi da quelli legittimi (phishing) o facilita forme di spionaggio informatico
c) la **violazione di comunicazioni private** (man in the middle, uomo nel mezzo) è un attacco informatico che consiste nell'interporsi di nascosto tra due persone che pensano di comunicare direttamente, ascoltando o leggendo le loro comunicazioni ed eventualmente modificandole.

3.2.3 Comprendere il termine "hotspot personale".

Per connettersi a Internet in assenza di reti cablate o Wi-Fi sicure è possibile utilizzare la rete dati di uno

smartphone attivando un **hotspot personale**, che consiste nell'utilizzare lo smartphone come un Access Point Wi-Fi, sul quale impostare tutte le opzioni di sicurezza disponibili.

3.2.4 Attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici.

Tutti gli smartphone recenti dispongono della funzionalità di attivare un hotspot personale. Prima di utilizzare questa funzione è opportuno verificare che il proprio contratto col fornitore di connettività ammetta questa funzione e gli eventuali costi aggiuntivi, nonché la quantità di dati che sono ancora scaricabili, per evitare di rimanere senza dato che la quasi totalità delle connessioni dati 4G è a consumo.

Utilizzeremo come esempio uno smartphone con sistema operativo Android 8, ma in qualsiasi smartphone la procedura è simile. Nella sezione Connessioni delle Impostazioni è presente la possibilità di attivare o disattivare e impostare l'hotspot. Per **attivare un hotspot personale** sul proprio smartphone occorre fare tap sul cursore accanto alla scritta Hotspot Wi-Fi portatile.

Per **rendere sicuro** l'hotspot occorre fare tap sulla scritta Tocca per configurare e impostare il livello di sicurezza massimo disponibile e una password robusta; eventualmente nascondere il nome della rete (SSID).

Per **disattivare l'hotspot personale** occorre fare nuovamente tap sul cursore accanto alla scritta Hotspot Wi-Fi portatile nella sezione Connessioni delle Impostazioni.

Per **connettere un dispositivo all'hotspot** occorre effettuare la ricerca della rete wireless attivata dall'hotspot tramite l'applet del sistema operativo in uso.

In ambiente Windows 10:

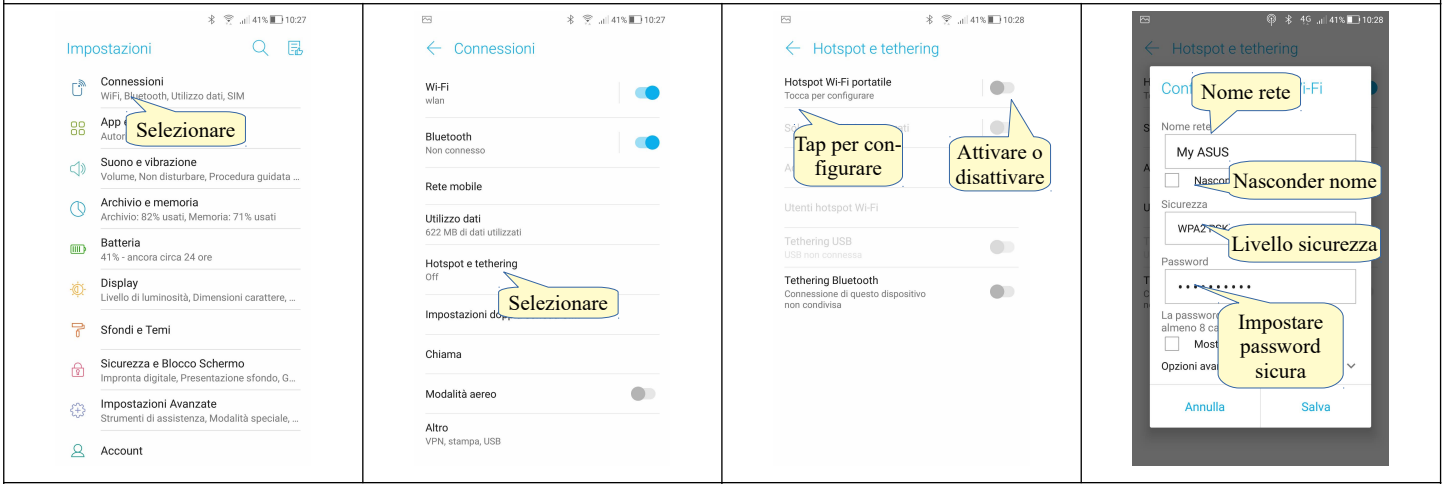
a) cliccare sull'icona Rete nella barra delle applicazioni
b) selezionare la rete corrispondente all'SSID dell'hotspot e cliccare su Connetti
c) digitare la password.

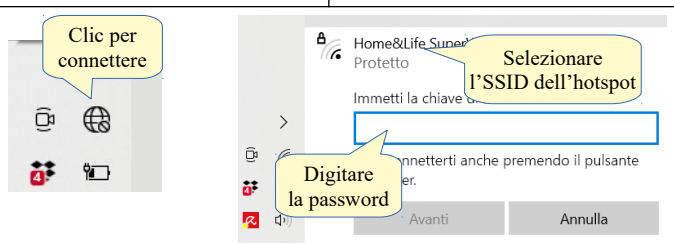
In ambiente Ubuntu 18.04:

a) cliccare sull'icona Impostazioni nella barra in alto
b) selezionare la rete corrispondente all'SSID dell'hotspot e cliccare su Connetti
c) digitare la password.

Per **disconnettere un dispositivo dall'hotspot** in ambiente Windows 10 occorre procedere come per la connessione, ma cliccare il pulsante Disconnetti. In ambiente Ubuntu non è presente l'opzione Disconnetti, pertanto occorre spegnere la scheda di rete Wi-Fi cliccando su Spegni, e riattivarla in caso di nuova connessione.

Attivazione hotspot in un dispositivo Android 8





Connessione alla rete Wi-Fi in Windows 10

Connessione alla rete Wi-Fi in ambiente Ubuntu 18.04

4 Controllo di accesso

4.1 METODI

4.1.1 Identificare i metodi per impedire accessi non autorizzati ai dati, quali: nome utente, password, PIN, cifratura, autenticazione a più fattori.

Per motivi di sicurezza, come indicato nei paragrafi precedenti, è opportuno che l'accesso ai dati presenti su un dispositivo o in un server locale o remoto sia possibile solo agli utenti autorizzati.

Per **impedire accessi non autorizzati** occorre che ciascun utente autorizzato disponga di credenziali che lo identifichino univocamente e che vengono richieste per poter accedere al dispositivo, alla rete, a uno dei servizi messi a disposizione da un server locale o remoto (sito web, posta elettronica, ecc...):

a) il **nome utente** identifica il singolo utente con un nome o con l'indirizzo email
b) la **password** è associata al nome utente e deve inserita insieme a esso per poter accedere ai dati. Per essere efficace la password deve rispondere a opportuni criteri di sicurezza (vedi punto 4.2.1)
c) il **PIN** (Personal Identification Number, numero di identificazione personale) è un codice formato generalmente da 4-6 cifre che deve essere inserito in aggiunta ad altri metodi di autenticazione (carte di debito o di credito, sim telefoniche, ecc…)
d) la **cifratura** dei dati consiste nel renderli illeggibili a chi non dispone della chiave di decifrazione (vedi punto 1.4.2)
e) l'**autenticazione a più fattori** consiste nell'utilizzare contemporaneamente per verificare l'identità dell'utente un dato che si conosce (password, PIN), un oggetto che si possiede (smartcard, app sul telefono, ecc…) e una caratteristica biometrica (impronta digitale, riconoscimento facciale, ecc…).

4.1.2 Comprendere il termine "one-time password" e il suo utilizzo tipico.

Per **One Time Password (OTP)** si intende una password temporanea e valida solo una volta, da cui il nome, che viene generata dal server a cui si richiede l'accesso e inviata all'utente su un canale diverso rispetto a quello utilizzato per l'accesso e sicuro, generalmente il telefono, tramite SMS o apposita app.

Questa modalità è più sicura rispetto all'utilizzo di una password standard, pertanto viene utilizzata per l'accesso o servizi che mettono a disposizione dati sensibili (es. il fascicolo sanitario personale) o di carattere finanziario (es. applicazioni di Internet Banking). Tuttavia da qualche tempo anche alcuni servizi di posta elettronica (es. Google mail) danno la possibilità di utilizzare questa modalità di autenticazione.

4.1.3 Comprendere lo scopo di un account di rete.

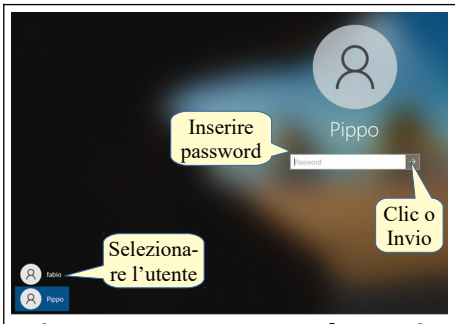
Lo **scopo di un account di rete**, oltre alla sicurezza necessaria alla protezione dei dati, è di assegnare a ciascun utente tutte e solo le risorse di rete necessarie.

Ad esempio ciascun utente e gruppo di lavoro necessita di poter accedere a determinate cartelle e file, ma non è opportuno che acceda a cartelle e file di altri utenti e gruppi di lavoro. Ciò vale anche per altre risorse di rete, come stampanti, servizi (accesso a internet, posta elettronica, ecc…).

4.1.4 Comprendere che per accedere alla rete sono necessari un nome utente e una password, e che è importante disconnettere l'account, al termine del collegamento.

Le risorse di rete vengono assegnate dall'amministratore di rete agli utenti e ai gruppi in base alle necessità di ciascuno, e agli utenti vengono concesse quelle di spettanza nel momento dell'autenticazione.

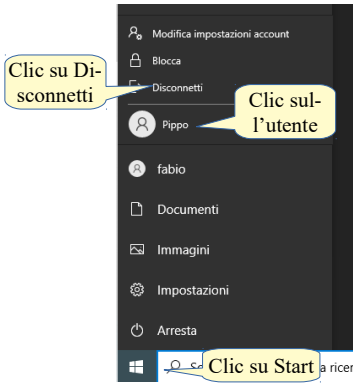
Pertanto quando si accede a una rete **ogni singolo utente dispone di un nome utente e di una password** che lo identificano univocamente dagli altri e che gli assegnano le risorse di sua competenza all'atto dell'autenticazione.



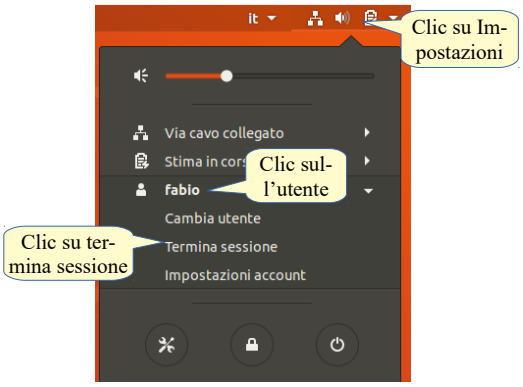
Autenticazione in Windows 10

Autenticazione in Ubuntu 18.04

Al **termine del collegamento alla rete è importante disconnettere l'account** per evitare che le risorse di propria competenza possano essere utilizzate da altri, in particolare se il computer è condiviso.



Disconnessione in Windows 10



Disconnessione in Ubuntu 18.04

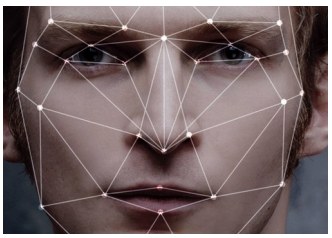
4.1.5 Identificare le comuni tecniche di sicurezza biometrica usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano.

Nell'autenticazione a più fattori (vedi punto 4.1.1) vengono utilizzati diversi possibili **tecniche di sicurezza biometrica** per identificare univocamente gli utenti:

a) le **impronte digitali** vengono analizzate tramite appositi sensori presenti su molti dispositivi come smartphone e notebook, oppure con periferiche esterne su computer desktop. Il sistema operativo dispone di un'apposita applet per impostare le impronte autentiche dell'utente e le riconosce in fase di autenticazione
b) la **scansione dell'occhio** (dell'iride) avviene tramite la fotocamera di alcuni smartphone; il sistema operativo dispone di un'applet per memorizzare l'iride dell'utente che riconosce in fase di autenticazione
c) il **riconoscimento facciale** ha un funzionamento simile al precedente e funziona su diversi smartphone
d) la **geometria della mano** utilizza diverse caratteristiche della mano (misure della mano, lunghezza delle dita, curvature del palmo) univoche per ciascun utente; questa tecnica richiede un dispositivo di analisi di maggiori dimensioni pertanto non viene utilizzato normalmente per l'accesso a un dispositivo o alla rete quanto per impianti fissi come sistemi di antifurto nelle abitazioni
e) l'**impronta vocale** utilizza il microfono di un dispositivo come smartphone e notebook, e il sistema operativo mette a disposizione un'applet per l'impostazione dell'impronta vocale e il suo riconoscimento in fase di autenticazione


Sensore impronte digitali

Scansione dell'iride


Riconoscimento facciale


Geometria della mano

4.2 GESTIONE DELLE PASSWORD

4.2.1 Riconoscere buone linee di condotta per la password, quali scegliere le password di lunghezza adeguata e contenenti un numero sufficiente di lettere, numeri e caratteri speciali; evitare di condividerle, modificarle con regolarità, scegliere password diverse per servizi diversi.

La password è uno dei modi per garantire la sicurezza dei dati e delle reti. Ciò è vero ma solo a condizione che la password venga gestita in modo corretto e risponda a criteri di robustezza.

Delle **buone linee di condotta per la password** sono:

a) deve **rispondere a criteri di robustezza**, con i quali si intende:

- una lunghezza di almeno 8 caratteri
- utilizzare sia lettere maiuscole che lettere minuscole
- utilizzare numeri arabi
- utilizzare caratteri speciali, come la @, il #, uno spazio vuoto (dove ammesso) o simili

b) **non deve essere condivisa** per nessun motivo (è importante però annotarla in un luogo sicuro per evitare che venga dimenticata o persa)
c) **deve essere modificata con regolarità**, per evitare che qualcuno possa venirne a conoscenza utilizzando una delle tecniche viste in precedenza (shoulder surfing, malware, ingegneria sociale)
d) **non si deve utilizzare la stessa password per account diversi** perché, nel caso venisse individuata, potrebbe essere utilizzata per tutti i servizi.

4.2.2 Comprendere la funzione e le limitazioni dei software di gestione delle password.

Per ricordare tutte le password si può utilizzare un software studiato per questo scopo. Il funzionamento di questi software consiste nel salvare le password utilizzate in un database interno cifrato per visualizzare il quale occorre utilizzare un'unica password, detta Master password.

Un esempio open source di software di questo tipo è Keepass, che esiste in versione Windows, Linux e Mac, oltre a versioni non ufficiali per i sistemi operativi per dispositivi mobili. È un software semplice da utilizzare anche su più dispositivi in quanto esiste anche un versione portable (senza necessità d'installazione) che si può copiare su una pen-drive. Inoltre è possibile esportare il database in altri formati.

Il limite di software è che, se qualcuno dovesse scoprire la Master password, può facilmente venire a conoscenza di tutte le password memorizzate.

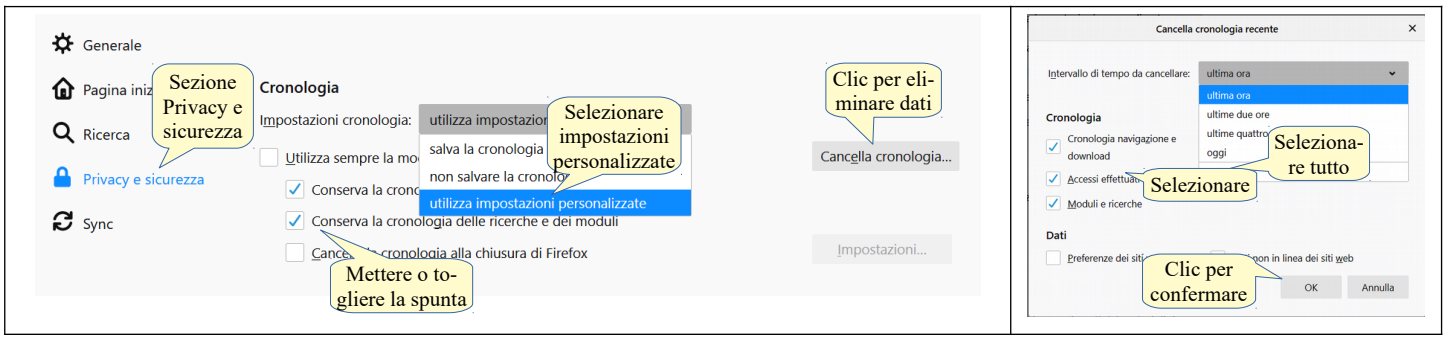
5 Uso sicuro del web

5.1 IMPOSTAZIONI DEL BROWSER

5.1.1 Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.

Per **attivare nel browser Firefox il completamento e il salvataggio automatico** dei dati che si inseriscono in un modulo occorre accedere alle impostazioni cliccando sul menu principale, selezionare la sezione Privacy e sicurezza > Cronologia e selezionare la voce Utilizza impostazioni avanzate nel menu a discesa. Fatto ciò occorre spuntare la voce Conserva la cronologia delle ricerche e dei moduli.

Per **disattivare il completamento e il salvataggio automatico** occorre togliere il segno di spunta: ciò fa sì che i dati inseriti nei campi dei moduli non vengano salvati né utilizzati per il completamento automatico.



5.1.2 Eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di internet, password, cookie, dati per il completamento automatico.

Per **eliminare i dati già inseriti** occorre accedere alla sezione Privacy e sicurezza > Cronologia delle impostazioni, cliccare su Cancella cronologia, spuntare i dati da cancellare e selezionare tutto nel menu a discesa Intervallo di tempo da cancellare.

5.2 NAVIGAZIONE SICURA IN RETE

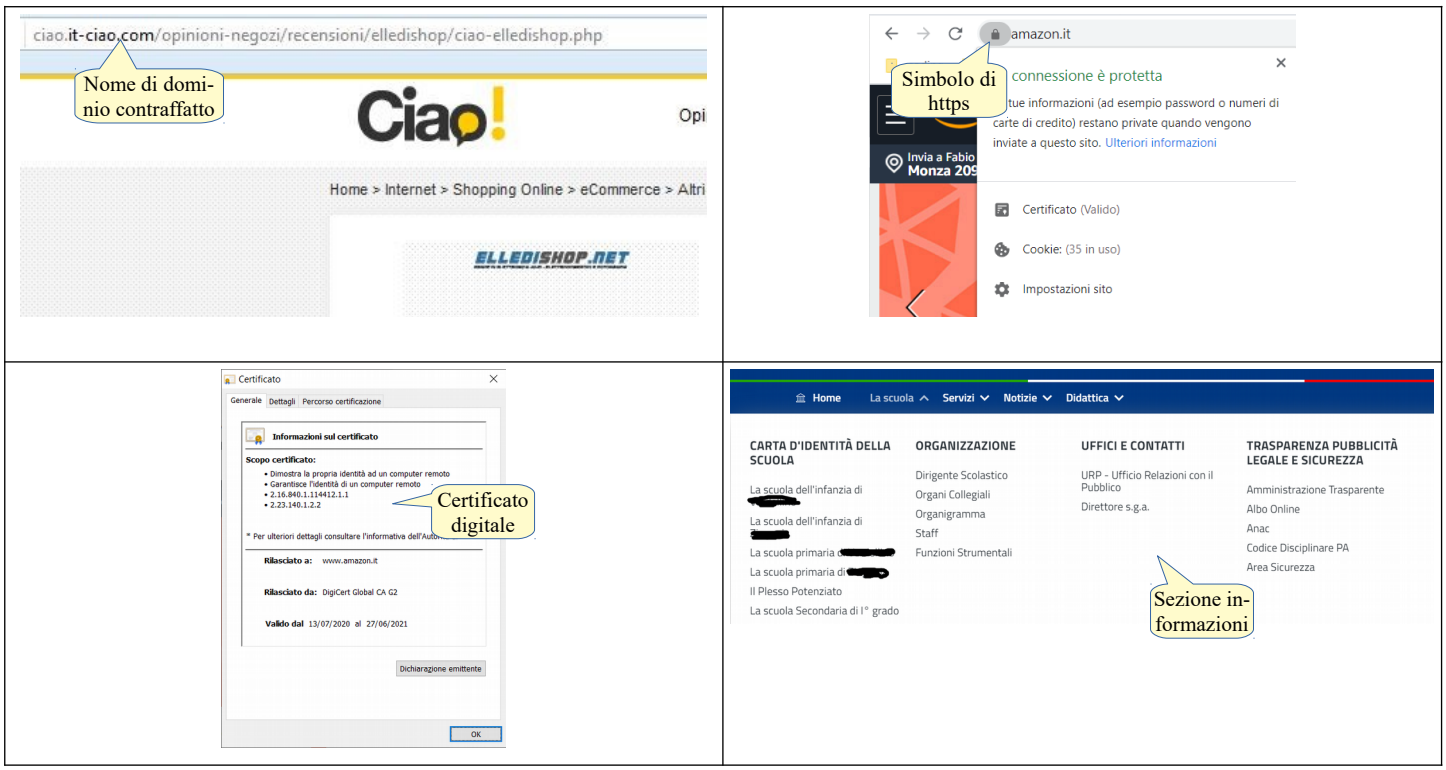
5.2.1 Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura.

Per evitare che qualche malintenzionato venga a conoscenza di dati riservati come le credenziali di accesso alla posta elettronica, a siti di e-commerce, a siti che permettono di effettuare transazioni finanziarie (home-banking) e a siti che contengono dati personali sensibili (fascicolo sanitario personale) è essenziale che ci si accerti che le **pagine web siano sicure**, cioè cifrate con l'utilizzo del protocollo https al posto del http, e che si stia utilizzando **una rete sicura** per la connessione a Internet (vedi punti 3.2.1 e seguenti).

5.2.2 Identificare le modalità con cui confermare la autenticità di un sito web, quali: qualità del contenuto, attualità, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio.

Spesso per appropriarsi di dati personali i malintenzionati realizzano siti copia di siti web reali, per esempio quello di una banca. Occorre pertanto verificare e **confermare l'autenticità di un sito web** attraverso i seguenti indicatori:

a) la **qualità del contenuto** di un sito web contraffatto spesso è scarsa, la lingua utilizzata a volte è poco corretta soprattutto se il clone è realizzato da hacker non italiani madrelingua
b) un sito web con **dati non aggiornati** non è particolarmente affidabile, per cui potrebbe essere non sicuro
c) l'**URL** della Homepage del sito contraffatto è differente da quella ufficiale del sito autentico, per cui è opportuno verificarla nella barra dell'indirizzo del browser
d) le **informazioni di contatto** possono essere trovate nella sezione Contatti del sito web e verificate con una ricerca su Internet
e) il **certificato di sicurezza** è un certificato digitale che attesta l'autenticità di un sito web da parte di un'autorità preposta e che può essere visualizzato nella barra dell'indirizzo di un browser
f) uno strumento molto efficace per verificare l'autenticità di un sito web è utilizzare un software o un servizio web di Whois, un protocollo di rete che permette, interrogando dei database server, d'**individuare l'intestatario** di un dominio e molte altre informazioni.



5.2.3 Comprendere il termine "pharming".

Il pharming è una tecnica per certi aspetti simile al phishing ma più sofisticata in quanto fa sì che, digitando l'indirizzo di un sito web lecito, si venga diretti verso un altro sito web, identico a quello lecito ma falso. Se

questo sito clonato richiede l'immissione di dati personali, questi verranno comunicati dall'utente inconsapevolmente e potranno poi essere utilizzati a suo danno.

Premesso che i siti web vengono identificati dal loro indirizzo IP, quando si digita un indirizzo alfanumerico questo viene tradotto nel corrispondente IP da un server DNS (Domain Name System): per esempio l'indirizzo IPv4 di aicanet.it è 52.30.215.78.

La tecnica del pharming modifica il riferimento e fa sì che l'indirizzo alfanumerico corrisponda a un IP diverso. L'utente non ha strumenti per rendersi conto della differenza se non controllare il certificato digitale di una pagina che utilizza il protocollo https.

5.2.4 Comprendere la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.

Nel web sono presenti siti che possono essere considerati inadatti a determinate categorie di utenti per motivi differenti: perdita di tempo e occupazione di banda nelle aziende (social media, streaming audio e video, ecc...), contenuti inadatti per bambini e minori (pornografia, violenza, razzismo, ecc…).

Per questo motivo sono stati realizzati software che filtrano i contenuti dei siti web impedendo l'accesso a quelli considerati inadatti.

Nelle aziende generalmente questi software vengono installati dall'amministratore su appositi apparati di rete che possono essere impostati in base ai criteri scelti e **filtrano i contenuti** in vari modi:

a) bloccando siti web in base al nome di dominio o all'indirizzo IP
b) impedendo l'utilizzo di porte utilizzate per servizi di streaming
c) impedendo il download di determinati tipi di file
d) filtrando i contenuti in base a parole chiave presenti nelle pagine web.

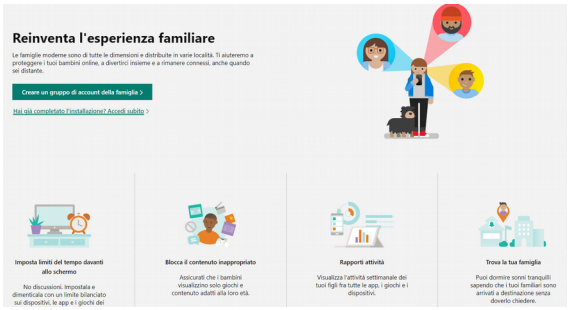
Nelle famiglie o in altre realtà come le scuole sono diffusi software di **controllo parentale** che impediscono l'accesso a contenuti inadatti a minori, la navigazione al di fuori degli orari stabiliti, fa un report delle attività su Internet, ecc... I principali sistemi operativi sia per computer che per dispositivi mobili dispongono di software integrati a questo scopo.

Windows family safety è un servizio online che, con la creazione di un gruppo di utenti membri di una famiglia, permette per ciascuno di essi di filtrare i contenuti, d'impostare dei limiti di tempo per la navigazione e di ricevere dei rapporti sull'attività.

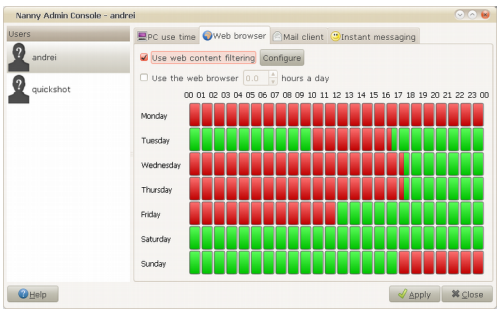
Ubuntu 18.04 non dispone di un software integrato ma è possibile installare un software come Gnome Nanny, che svolge funzioni simili.

Mac OSX permette di attivare il controllo parentale dalle preferenze di sistema.

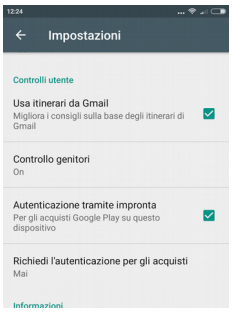
Il controllo parentale è possibile anche per mezzo dei sistemi operativi per dispositivi mobili Android e iOS.



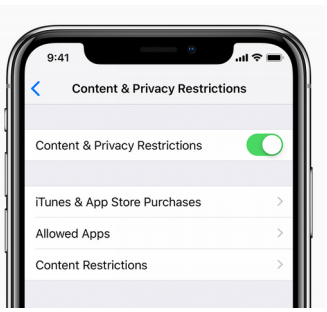
Windows family safety



Gnome nanny



Android



iOS

6 Comunicazioni

6.1 POSTA ELETTRONICA

6.1.1 Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica.

La posta elettronica ordinaria (PEO) è un mezzo di comunicazione non sicuro in quanto i messaggi vengono inviati in chiaro, senza nessuna codifica. Per fare un paragone con la posta tradizionale, l'invio di un messaggio di posta elettronica può essere considerato non tanto una lettera in busta chiusa, quanto una cartolina postale.

Per rendere l'invio di un messaggio sicuro, occorre pertanto cifrare il messaggio stesso, in modo che solo il legittimo destinatario, in possesso di una chiave di decodifica, sia in grado di leggerlo. Cifrare un messaggio di posta elettronica equivale a inserirlo in una busta e chiuderla prima d'inviarlo.

6.1.2 Comprendere il termine firma digitale.

La Firma Digitale è l'equivalente informatico di una tradizionale firma autografa apposta su carta e ha le seguenti caratteristiche:

a) Autenticità, che garantisce l'identità del sottoscrittore
b) Integrità, che assicura che il documento non sia stato modificato dopo la sottoscrizione
c) Validità legale, che attribuisce pieno valore legale al documento firmato.

La firma digitale è costituita da un dispositivo (smartcard o chiavetta USB) che contiene un certificato digitale di sottoscrizione, tramite il quale il titolare può firmare digitalmente i propri documenti.

6.1.3 Identificare i possibili messaggi fraudolenti o indesiderati.

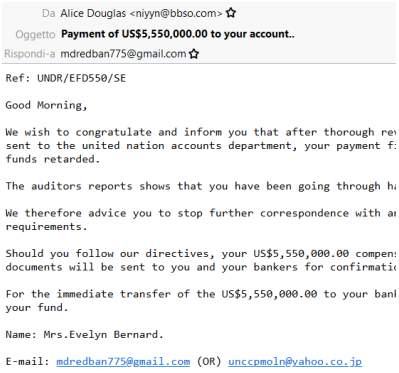
La posta elettronica è uno strumento spesso usato in modo non corretto da parte di malintenzionati per trarne vantaggio economico o per carpire informazioni riservate.

Un esempio di utilizzo scorretto della posta elettronica è la cosiddetta **spam**, cioè l'invio di messaggi non richiesti, generalmente di carattere pubblicitario, che hanno lo scopo d'indurre i destinatari ad acquistare qualcosa.

Un altro esempio è il **phishing**, cioè l'invio di messaggi fraudolenti che inducono i destinatari a fornire inconsapevolmente a chi li ha inviati dati riservati, allo scopo di frode.

In tutti i casi è opportuno non aprire e soprattutto non rispondere a messaggi di questi tipo, neppure per dire che non si è interessati, perché in tal modo si confermerebbe che l'indirizzo email in questione è attivo e viene utilizzato, invogliando gli spammer (chi invia messaggi spam) o i phisher (chi invia messaggi di phishing) a inviare sempre più messaggi all'indirizzo in questione.

Messaggio di Spam



Messaggio di Phishing

6.1.4 Identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali.

Il phishing ha diverse caratteristiche presenti singolarmente o più spesso insieme che permettono di riconoscere messaggi di questo tipo:

a) il mittente viene camuffato con **nomi di persone o di aziende autentiche** per indurre il destinatario a una maggiore fiducia nei contenuti del messaggio fraudolento
b) nel corpo del messaggio sono presenti **collegamenti a falsi siti web** che simulano quelli autentici e

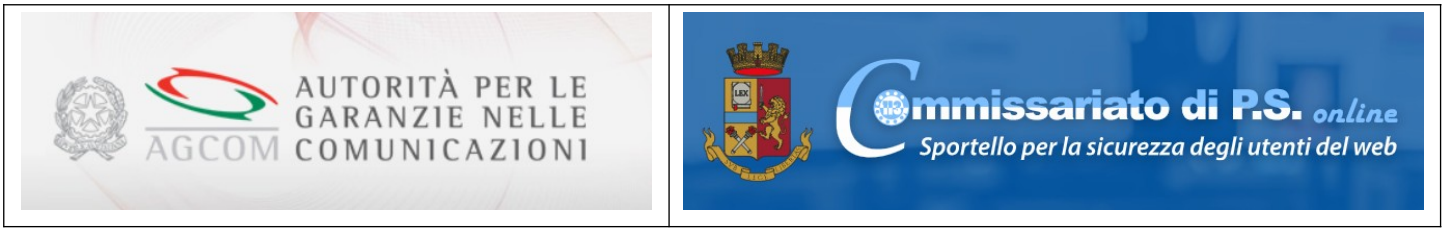
hanno lo scopo di vendere prodotti non originali o di carpire informazioni personali. Per riconoscere l'autenticità di un sito web, è sufficiente controllare l'URL dei link presenti nel messaggio

c) per essere più verosimili spesso i messaggi fraudolenti contengono immagini con **loghi e marchi aziendali falsi**
d) quando lo scopo dei messaggi fraudolenti è il furto d'identità (phishing) **il destinatario è incoraggiato a inserire i suoi dati personali** in moduli di siti web falsi con la minaccia che il suo account scade oppure con la promessa di vincere dei premi.

6.1.5 Essere consapevoli che è possibile denunciare tentativi di phishing alle organizzazioni competenti o alle autorità preposte.

I reati informatici possono essere denunciati alle organizzazioni competenti e alle autorità preposte.

L'autorità garante delle comunicazioni è l'AgCom, mentre l'autorità preposta alla tutela dei cittadini è la Polizia Postale. Oltre alla denuncia in presenza, entrambe queste autorità permettono la denuncia online.



6.1.6 Essere consapevoli del rischio d'infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.

Alcuni messaggi fraudolenti hanno **allegati infetti di tipo eseguibile oppure contenenti macro, che possono danneggiare il computer nel caso vengano aperti**.

Pertanto, in particolare in ambiente Windows che è più vulnerabile (vedi punto 2.2.1), ma anche con altri sistemi operativi per computer e per dispositivi mobili, occorre fare molta attenzione prima di aprire un allegato, per esempio facendo una scansione con il software antivirus.

6.2 RETI SOCIALI

6.2.1 Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.

Le reti sociali (social network) sono strumenti di comunicazione e gestione delle conoscenze molto diffusi al giorno d'oggi sia tra i giovani che tra gli adulti.

A volte questi strumenti vengono utilizzati in modo poco attento, dimenticando che tutto ciò che viene messo su internet diventa di pubblico dominio e di fatto se ne perde il controllo.

Per questo motivo è importante **non divulgare informazioni personali e dati riservati**, come l'indirizzo di casa, il numero di telefono o l'indirizzo email, le credenziali di accesso a servizi e sistemi informatici, PIN e qualsiasi altro dato. Anche la pubblicazione di immagini private dovrebbe essere considerata con attenzione, così come la divulgazione di idee e tendenze di carattere religioso, politico, sessuale.

Infatti tali informazioni potrebbero essere utilizzate per mettere in atto reati, per profilare l'utente e per minare la web reputation, con grave lesione della privacy e non solo.

6.2.2 Essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale, quali riservatezza dell'account e propria posizione.

Utilizzando le reti sociali è possibile impostare la privacy del proprio profilo. È importante sapere che esiste questa possibilità ed evitare di lasciare pubblico il proprio profilo, rendendolo accessibile solo a persone che si conoscono anche nella vita reale.

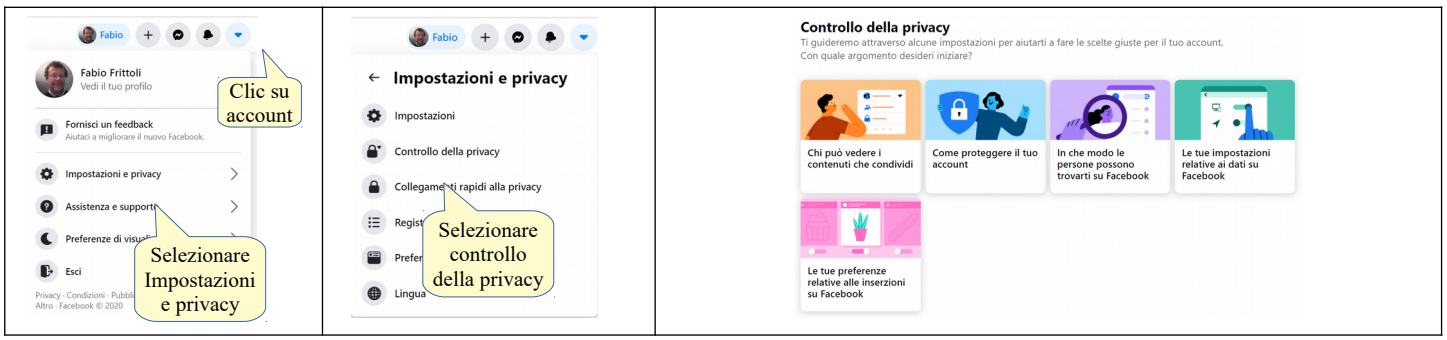
Nel corso del tempo le opzioni relative alla sicurezza del proprio account e alla tutela della privacy possono cambiare, oppure possono cambiare le proprie esigenze relative a questi temi, pertanto è opportuno **verificare con regolarità queste impostazioni**.

6.2.3 Applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione.

Per **modificare le opzioni di privacy** In Facebook, che utilizzeremo come esempio, occorre cliccare sul pulsante Account, scegliendo Impostazioni e privacy > Controllo della privacy.

In questo modo si accede a una pagina suddivisa in cinque sezioni che permettono d'impostare nel dettaglio tutte gli aspetti per la tutela della propria privacy (visibilità dei contenuti, protezione dell'account, rintracciabilità, protezione dei dati, inserzioni pubblicitarie) ciascuna delle quali può essere modificata per adattarla alle proprie esigenze.

a) La sezione ***Chi può vedere i contenuti condivisi*** permette d'impostare per ciascun tipo di contenuti le opzioni Solo io, Amici, Amici stretti, Tutti e anche di personalizzare in base alle singole persone.
b) La sezione ***Come proteggere l'account*** permette di cambiare la propria password e di utilizzare l'autenticazione a due livelli, oltre che d'impostare gli avvisi in caso di accessi sospetti.
c) La sezione ***In che modo le persone possono trovarti su Facebook*** permette di limitare agli Amici degli amici o lasciare libera la possibilità d'inviare richieste di amicizia, che possano essere utilizzati o meno l'email o il numero di telefono come criterio di ricerca, che si possa essere cercati anche tramite motori di ricerca
d) La sezione ***Le tue impostazioni relative ai dati su Facebook*** permette di modificare le impostazioni relative alle applicazioni o siti web per i quali si è utilizzato l'account di Facebook, e di accettare o meno che Facebook effettui il riconoscimento facciale per trovarti in fotografie
e) La sezione ***Le tue preferenze relative alle inserzioni su Facebook*** permette a Facebook di utilizzare o meno i dati del proprio profilo per personalizzare le inserzioni pubblicitarie.



È importante essere consapevoli che è opportuno impostare con cura la privacy per proteggersi da furti d'identità e di dati, e per proteggere la propria reputazione web.

6.2.4 Comprendere i pericoli potenziali connessi all'uso di siti di reti sociali, quali cyberbullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli

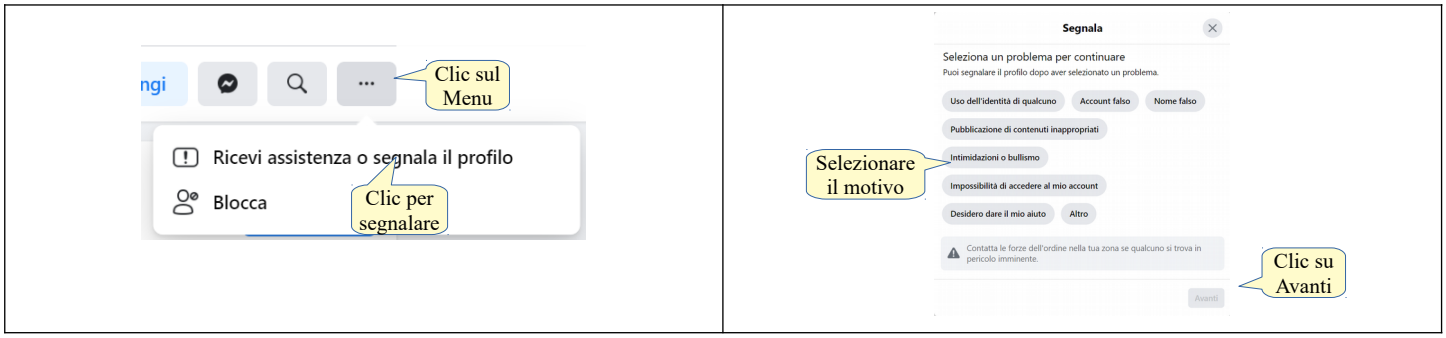
Chi utilizza le reti sociali, infatti, può essere vittima di diversi tipi di attacco:

a) il **cyberbullismo** consiste nell'utilizzo di internet per attaccare ripetutamente un individuo in diversi modi, tra cui:
   – flaming: messaggi online violenti e volgari
   – molestie: spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno
   – denigrazione: sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione
   – sostituzione di persona: farsi passare per un'altra persona
   – inganno: ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni confidate via mezzi elettronici
   – esclusione: escludere deliberatamente una persona da un gruppo online
   – cyberpersecuzione: molestie e denigrazioni ripetute e minacciose mirate a incutere paura
   – doxing: diffusione pubblica via internet di dati personali e sensibili
b) l'**adescamento** (grooming) consiste nel tentativo da parte di un "predatore" di acquisire la confidenza di una giovane vittima sfruttando le sue debolezze psicologiche
c) la **diffusione di informazioni personali** private e a volte imbarazzanti come nel caso del revenge porn (pubblicazione di immagini o video sessualmente espliciti)
d) le **false identità**, dette anche Fake, consistono nel creare falsi profili su una rete sociale e vengono spesso usate per tentativi di adescamento e anche per il cyberbullismo
e) i **link o messaggi fraudolenti**, detti anche phishing, hanno lo scopo di carpire informazioni basandosi

sull'ingegneria sociale.

6.2.5 Essere consapevoli che è possibile denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte.

Le reti sociali danno la possibilità di segnalare usi e comportamenti inappropriati da parte di qualche utente. Prendendo come esempio Facebook, per segnalare un utente occorre selezionare il profili dell'utente da bloccare, cliccare sull'icona del menu e selezionare Ricevi assistenza o segnala un profilo. Nella finestra che si apre occorre selezionare uno dei motivi indicati e cliccare su Avanti e poi su Fine.



6.3 VOIP E MESSAGGISTICA ISTANTANEA

6.3.1 Comprendere le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP), quali malware, accesso da backdoor, accesso a file, intercettazione (eavesdropping).

Come la posta elettronica, anche la messaggistica istantanea e le chiamate VoIP comportano alcuni rischi che possono compromettere la sicurezza del proprio dispositivo e dei propri dati:

a) alcuni **malware** (spesso si tratta di Trojan horse) si diffondono tramite applicazioni come Messenger o Skype e hanno principalmente lo scopo di diffondere spam
b) diversi software di messaggistica e videochiamate come Skype e WhatsApp sono stati accusati di contenere delle **backdoor** in grado di spiare gli utenti a scopi commerciali
c) le vulnerabilità di diverse applicazioni per la videoconferenza, ad esempio Zoom, possono permettere a malintenzionati di **accedere ai propri file**
d) per altre vulnerabilità possono anche esserci **intercettazioni delle comunicazioni** private (eavesdropping) in corso tra gli utenti di applicazioni come WhatsApp e Messenger.

Se la vulnerabilità dipende da malware è possibile difendersene utilizzando software antivirus e tenendo aggiornati software, ma quando dipendono dal fornitore del servizio non ci sono difese, se non quella di scegliere l'applicazione più sicura, per esempio per le videoconferenze si potrebbe utilizzare il software libero e open source Jitsi ospitato su server sicuri e pubblici.

6.3.2 Riconoscere i metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP (Voice over IP), quali cifratura, non divulgazione di informazioni importanti, limitazione alla condivisione di file.

Come per la posta elettronica e le reti sociali, per ridurre il rischio d'infezioni e di perdita di dati personali, è opportuno ricorrere a metodi di cifratura delle comunicazioni, ma anche stare attenti a non divulgare informazioni personali e file attraverso questi mezzi.

Inoltre, come per gli allegati della posta elettronica, occorre stare attenti quando si apre un file ricevuto da altre persone tramite un programma di messaggistica istantanea.

6.4 DISPOSITIVI MOBILI

6.4.1 Comprendere le possibili implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti.

Le **app per dispositivi mobili, per motivi di sicurezza e controllo della qualità delle stesse, vengono normalmente installate attraverso dei negozi online (app store) ufficiali**, direttamente controllati e gestiti dai produttori dei sistemi operativi, Google Play per Android e App Store per iOS.

È tuttavia possibile utilizzare negozi online alternativi oppure effettuare direttamente il download dell'app dal sito web del produttore, ma è opportuno verificare bene che si tratti di app store o app affidabili. Un esempio di app store alternativo a Google Play ma affidabile e basato su un progetto open source è Fdroid, mentre recentemente, a causa del blocca dei servizi Google nei confronti di Huawei, è stato realizzato lo store alternativo AppGallery per i suoi dispositivi.

Se si installa un'app non sicura sul proprio dispositivo mobile si può andare incontro a vari tipi di problemi:

a) alcune app contengono **malware** e, in tal caso, l'app può essere considerata un trojan
b) altre app possono utilizzare molte risorse del dispositivo, rendendolo meno utilizzabile
c) in alcuni casi le app non sicure possono accedere a dati personali, comportandosi come spyware
d) spesso le applicazioni provenienti da store non ufficiali possono essere bassa qualità oppure avere costi nascosti.

6.4.2 Comprendere il termine "autorizzazioni dell'applicazione".

Le app per dispositivi mobili la prima volta che vengono avviate chiedono l'**autorizzazione a utilizzare alcune risorse del dispositivo**, necessarie al suo utilizzo. Per esempio un'app di Instant Messaging e per videoconferenza chiederà l'autorizzazione a utilizzare il microfono e la camera del dispositivo, ma anche la rubrica dei contatti per facilitare la comunicazione con persone che dispongono di account con quella stessa app. Un'app di navigazione o di ricerca di esercizi commerciali, chiederà l'autorizzazione a utilizzare il posizionamento GPS.

6.4.3 Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini.

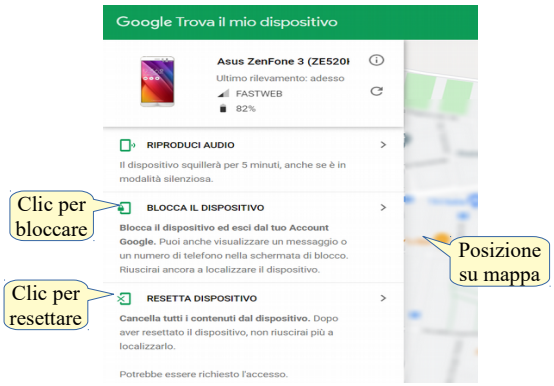
È necessario essere consapevoli che, dando queste autorizzazioni, si permette all'app di conoscere molti dati personali e di facilitare la possibilità che, in caso di backdoor o altri malware, possano essere utilizzate da malintenzionati. Pertanto è opportuno, prima di dare queste autorizzazioni, verificare che siano tutte legittimamente necessarie all'app che le richiede e che l'app che stiamo autorizzando sia sicura.

6.4.4 Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo.

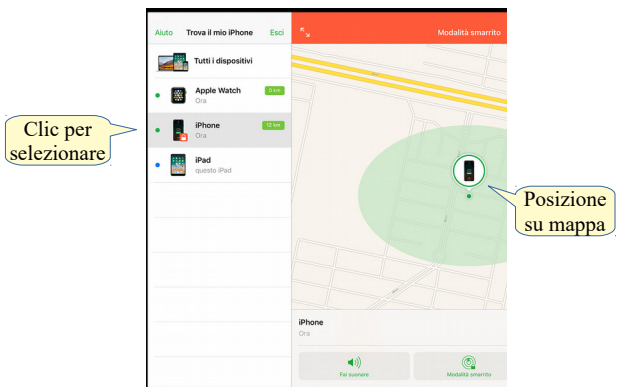
I sistemi operativi per dispositivi mobili Android e iOS dispongono di sistemi per **localizzare il dispositivo smarrito o rubato ed eventualmente per bloccarlo o cancellare i dati da remoto**. Per poter attivare queste possibilità occorre che il telefono sia acceso e che abbia una connessione dati.

In ambiente Android occorre accedere alla pagina web https://android.com/find e accedere con l'account utilizzato su tutti i dispositivi collegati all'account, e si può selezionare quello da ritrovare. Fatto ciò viene attivato da remoto il GPS del **telefono che viene localizzato** e mostrato in una mappa; nella stessa pagina si trova anche la possibilità di **bloccare il telefono o di resettarlo**.

In ambiente iOS occorre accedere alla pagina https://www.icloud.com/find e accedere con l'account utilizzato su tutti i dispositivi collegati all'account, e si può selezionare quello da ritrovare. Fatto ciò viene attivato da remoto il GPS del **telefono che viene localizzato** e mostrato in una mappa; nella stessa pagina si trova anche la possibilità di **bloccare il telefono o di resettarlo**.



Localizzazione, blocco e reset in ambiente Android



Localizzazione, blocco e reset in ambiente iOS

7 Gestione sicura dei dati

7.1 MESSA IN SICUREZZA E SALVATAGGIO DI DATI

7.1.1 Riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, quali non lasciarli incustoditi, registrare la collocazione e i dettagli degli apparati, usare cavi antifurto, controllare gli accessi alle sale dei computer.

Per far sì che i dati non vengano persi o rubati, prima di tutto è necessario che **i dispositivi informatici siano messi in sicurezza, cioè che non vengano sottratti o smarriti**. Per farlo occorre prestare attenzione a:

a) che i **computer, in particolare quelli portatili, e i dispositivi mobili non siano lasciati incustoditi** dai proprietari e, in caso di assenza, vengano messi sotto chiave
b) tenere traccia della **collocazione dei dispositivi**, così come dei loro dettagli, in modo da poter verificare in modo preciso eventuali mancanze
c) utilizzare, in particolare per notebook e computer desktop predisposti, **i cavi di sicurezza**, tra cui i più diffusi seguono lo standard Kensington Security Lock.
d) controllare gli **accessi ai locali nei quali i dispositivi sono collocati**, in modo da poter più facilmente risalire all'autore di eventuali furti.

7.1.2 Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati da computer e da dispositivi mobili.

Si possono perdere i dati non solo in caso di furto, ma anche per la rottura di un dispositivo di memorizzazione o a causa di eventi naturali come alluvioni, incendi, terremoti che danneggino o distruggano computer e dispositivi mobili.

È quindi importante **avere una copia di sicurezza (backup) dei dati** aggiornata e facilmente riutilizzabile che permetta di ripristinarli in caso di perdita.

Tra i dati da salvare nella copia di sicurezza vanno compresi i file realizzati in proprio (documenti, immagini, ecc...), le informazioni di carattere finanziario, i segnalibri e la cronologia salvati nel browser.

7.1.3 Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione del supporto dei dati salvati, compressione dei dati.

Affinché sia davvero utile, è necessario che la copia di sicurezza dei dati abbia determinate caratteristiche:

a) una **copia di sicurezza dei dati serve se è aggiornata e regolare**
b) pertanto occorre, in base al numero di documenti che vengono memorizzati ogni giorno nella memoria del dispositivo, **pianificare la frequenza** con cui la copia viene effettuata. Questa incombenza viene facilitata dai software che automatizzano questa operazione, che permettono di schedulare il backup
c) occorre prestare attenzione alla collocazione della copia di sicurezza: se la copia viene posta accanto al dispositivo, anch'essa corre il rischio di essere persa (furto, danneggiamento a causa di eventi, ecc...). **La copia di sicurezza va quindi posta in un luogo, il più sicuro possibile, diverso dall'originale**. Negli ultimi tempi per questo motivo sempre più spesso la copia dei sicurezza dei dati viene effettuata online, su server remoti
d) per ridurre lo spazio occupato e i tempi di esecuzione, è opportuno effettuare **la compressione dei dati** della copia di backup
e) per evitare che persone non autorizzate possano accedere ai dati presenti nella copia di sicurezza, è opportuno utilizzare un sistema di cifratura con richiesta di password nel momento del ripristino.

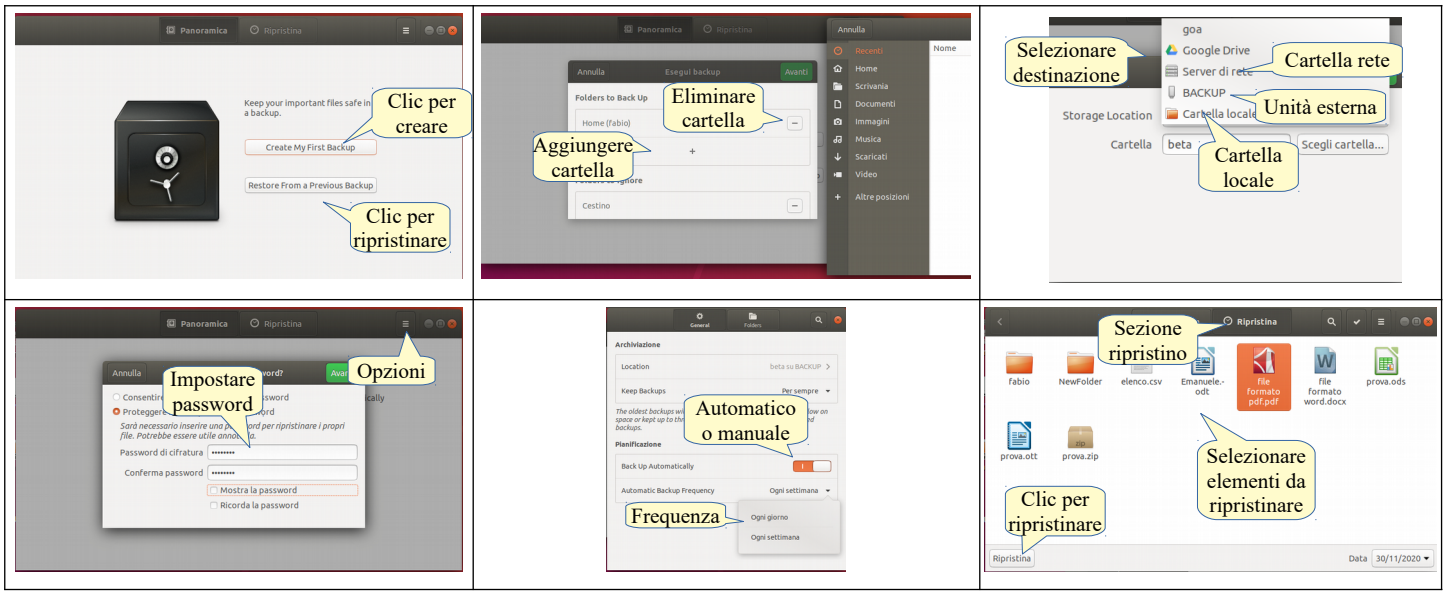
Ultimamente, grazie alla diffusione di connessioni veloci a Internet e ai costi ridotti dei servizi cloud, le copie di sicurezza spesso vengono fatte tramite software di sincronizzazione che mantengono identici file e cartelle locali e remoti.

7.1.4 Effettuare la copia di sicurezza di dati su un supporto quale: unità disco/dispositivo locale, unità esterna, servizio su cloud.

Per **effettuare la copia di sicurezza su un supporto locale o su una unità esterna** in ambiente Ubuntu 18.04 si può installare tramite Ubuntu software o linea di comando un software open source come per esempio Déjà Dup che si può utilizzare con un'interfaccia grafica davvero molto semplice.

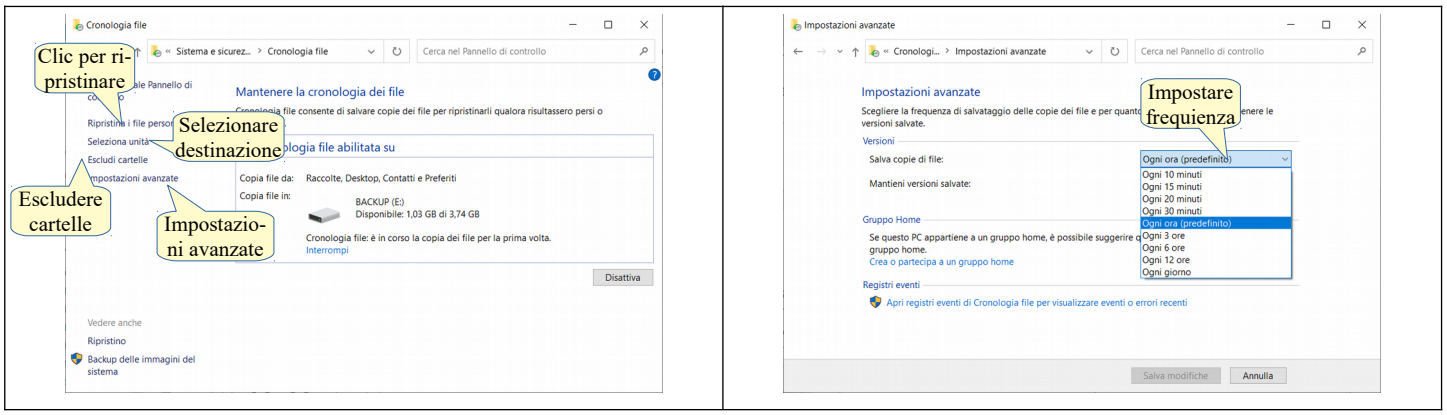
Occorre prima di tutto impostare il backup, cliccando su Create my first Backup, selezionare le cartelle da

copiare (nell'esempio la cartella home), il supporto locale o esterno (nell'esempio la pen-drive Backup), eventualmente impostare una password. Nelle impostazioni è possibile pianificare il backup con cadenza giornaliera o settimanale.



Per **effettuare la copia di sicurezza su una cartella di rete**, in fase di scelta della destinazione selezionare Server di rete. Per **effettuare la copia di sicurezza in cloud**, selezionare Google Drive. Prima di procedere al backup vengono richieste le credenziali di accesso al servizio e, ovviamente, deve essere attiva una connessione a Internet.

Per **effettuare la copia di sicurezza su un supporto locale o su una unità esterna** in ambiente Windows utilizzando l'applet di sistema occorre accedere alle Impostazioni > Aggiornamento e sicurezza > Backup. Cliccando su Visualizza Impostazioni avanzate è possibile modificare le cartelle da copiare, escludendo qualcuna di quelle predefinite (tutta la cartella dell'utente), il supporto locale o l'unità esterna su cui effettuare la copia e la frequenza.



Per **effettuare la copia di sicurezza su una cartella di rete**, in fase di scelta della destinazione cliccare su Aggiunta guidata risorse di rete, e poi selezionarla come unità di destinazione del backup. Per **effettuare la copia di sicurezza in cloud**, occorre utilizzare i software di sincronizzazione specifici, per esempio quello di OneDrive è già installato in Windows 10 ma ce ne sono per qualsiasi servizio cloud. Questi software sincronizzano una cartella locale con lo spazio di archiviazione remoto, pertanto per effettuare il backup basta impostarne la copia in questa cartella sincronizzata, in modo che vengono salvati in remoto in tempo reale, in presenza di una connessione a Internet.

7.1.5 Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud.

Per **ripristinare i dati da una copia di sicurezza su unità disco o dispositivo locale** occorre utilizzare l'apposita funzione di ripristino del software utilizzato per la creazione del backup.

In ambiente **Ubuntu 18.04** occorre:

a) avviare il software di backup

b) cliccare su Restore from a previous backup
c) selezionare il file e cartelle da ripristinare
d) inserire la password utilizzata eventualmente per la cifratura dei dati.

Per **ripristinare i dati da una copia di sicurezza su cartella di rete o in cloud** occorre svolgere le stesse operazioni precedenti e inserire le credenziali di accesso quando richieste.

In ambiente **Windows 10** occorre, dopo aver collegato l'eventuale unità esterna o inserito le credenziali di accesso a risorse di rete o in cloud, accedere a Impostazioni > Backup e cliccare su Ripristina i file da un backup corrente. Nella finestra cui si accede cliccare su Ripristina file personali. La copia dei file e delle cartelle sincronizzati nel cloud si trova nella cartella impostata per la sincronizzazione.

7.2 CANCELLAZIONE E DISTRUZIONE SICURA

7.2.1 Distinguere tra cancellare i dati ed eliminarli in modo permanente.

È importante essere coscienti del fatto che la semplice cancellazione di un file non garantisce la sua effettiva rimozione. Ciò per due motivi:

a) i moderni sistemi operativi dispongono di una cartella speciale, chiamata Cestino, dove vengono spostati i file cancellati. È pertanto possibile ripristinare dati cancellati in questo modo
b) anche se i file vengono cancellati dal Cestino, in realtà non vengono eliminati dal supporto di memoria di massa, ma solo resi invisibili al sistema operativo in quanto lo spazio da essi occupato viene segnalato come libero per essere occupato da altri file e cartelle. Pertanto, anche se non saranno visibili con gli strumenti di gestione file del sistema operativo, finché lo spazio che occupano non verrà sovrascritto da altri file e cartelle, con programmi specifici possono essere ricostruiti integralmente o quasi, a seconda del tempo che passa dalla loro cancellazione e dall'uso che viene fatto del computer.

7.2.2 Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili.

I **dati non più necessari, personali o di terzi, devono essere eliminati in modo permanente** dalle memorie di massa e soprattutto dai dispositivi mobili per proteggerli da possibili accessi e utilizzi da parte di malintenzionati.

In particolare è importante effettuare questa operazione sui dispositivi mobili, che possono più facilmente essere oggetto di furto. Le memorie di massa di qualsiasi dispositivo informatico dovrebbero essere cancellate in modo permanente prima di essere dismesse in quanto potrebbero essere essere oggetto di "information diving", cioè recuperate da malintenzionati per rubare i dati in esse contenuti (vedi punto 1.3.4).

7.2.3 Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente, come nel caso dei siti di reti sociali, blog, forum su internet, servizi su cloud.

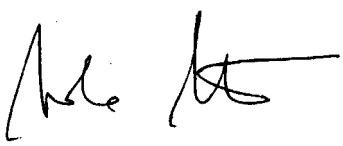
È importante sapere che i dati pubblicati su Internet, anche se eliminati dal proprietario, potrebbero essere stati scaricati da terzi ed essere successivamente utilizzati senza il consenso dell'autore, spesso a scopo di cyberbullismo, ma anche per verificare la reputazione web delle persone.

7.2.4 Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di software per la cancellazione definitiva dei dati.

Per cancellare definitivamente i dati è necessario pertanto utilizzare altri metodi:

a) per i documenti cartacei è opportuno utilizzare dei **trita-documenti**, che tagliano a striscioline o riducono a coriandoli i fogli
b) le memorie di massa da eliminare vanno rese inutilizzabili attraverso la **distruzione** fisica o la **smagnetizzazione** per mezzo di apparecchi (degausser) in grado di applicare intensi campi magnetici
c) se la memoria di massa deve essere riutilizzata è opportuno **eliminare i file in modo definitivo** e sicuro per mezzo di appositi software che sovrascrivono i file più volte in modo da renderli non recuperabili. Bleachbit è un software, disponibile sia per Windows che per Ubuntu, in cui si possono scegliere quali cartelle cancellare. Se si sceglie di cancellare in modo sicuro il Cestino, in file in esso contenuti saranno eliminati in modo sicuro. Se il Cestino è stato già svuotato, si può scegliere di cancellare in modo sicuro lo Spazio libero su disco.

L'autore, prof. Fabio Frittoli



NB=tutte le immagini utilizzate nella presente dispensa sono state realizzate in proprio o tratte da http://wikimediafoundation.org