ICDL
The Digital Skills Standard

AICA

ICDL IT-SECURITY

ICDL – IT-Security

Area di Riferimento: ICDL Workforce

ICDL - International Certification of Digital Literacy - è il nuovo nome per il programma ECDL, che riflette la natura globale delle competenze digitali, la rapida evoluzione della tecnologia e, soprattutto, sottolinea il suo valore internazionale e il nostro impegno per la qualità. Attraverso questo Programma, AICA vuole evidenziare la sua "missione culturale" di associazione no-profit che ha accompagnato la storia dell'ICT italiano fin dalle sue origini.

ICDL Workforce è un insieme di moduli destinati agli studenti e a chi già lavora per utilizzare, in modo efficace e certificato, programmi e strumenti che favoriscono e sostengono la produttività e l'innovazione.

Il modulo ICDL IT-Security è orientato all'acquisizione di concetti e allo sviluppo di competenze per identificare e affrontare le minacce digitali associate all'uso delle tecnologie informatiche, migliorando la capacità di proteggere i dati e garantirne la sicurezza, e consente di prepararsi al conseguimento della certificazione "ECDL/ICDL IT-Security".

Autore: Mario R. Storchi

www.aicanet.it, www.icdl.it, www.aicadigitalacademy.it www.edizionimanna.com

Sommario

INTRODUZIONE

Le competenze digitali sono necessarie per la nostra vita personale e professionale. **ICDL** ha progettato un programma di certificazioni riconosciute a livello internazionale, articolato secondo gli interessi e le esigenze di studenti, lavoratori, professionisti e, in generale, di tutti i cittadini che desiderano usare in modo consapevole e adeguato gli strumenti digitali e le loro applicazioni.

Questo manuale fa riferimento all'area **ICDL Workforce**, caratterizzata da un insieme di moduli destinati agli studenti e a chi già lavora per utilizzare, in modo efficace e certificato, programmi e strumenti che favoriscono e sostengono la produttività e l'innovazione. In particolare, il manuale **ICDL IT-Security** vi guida nell'acquisizione delle conoscenze e delle competenze per identificare e affrontare le minacce digitali associate all'uso delle tecnologie informatiche, migliorando la capacità di proteggere i dati e garantirne la sicurezza, come specificato nel *syllabus* **ICDL IT-Security**.

Le tecnologie informatiche vengono utilizzate da un numero sempre crescente di persone per svolgere una gamma sempre più ampia di attività, mettendo in gioco una mole di dati sempre maggiore: diventa quindi critica la necessità di garantire la sicurezza di tali dati. Tutti gli utilizzatori di tecnologie informatiche dovrebbero vigilare sulle minacce alla sicurezza IT – chiamata anche sicurezza informatica - quali virus, phishing, hacker, frodi on line e furti d'identità in generale. L'uso di prodotti di sicurezza IT, integrato con adeguate competenze e conoscenze che consentono di identificare e affrontare le minacce alla sicurezza IT, è il modo più efficace per proteggere sé stessi ed i propri dati.

Gli individui sono infatti vulnerabili tanto quanto lo sono i sistemi. Ogni catena è forte quanto il suo anello più debole, e in relazione alla sicurezza IT spesso sono le azioni dell'utente, piuttosto che qualsiasi carenza tecnologica, che compromettono la sicurezza di un computer personale o - per esempio, nei luoghi di lavoro - la sicurezza di una intera rete aziendale. Pertanto, la sicurezza delle informazioni deve essere rafforzata attraverso la consapevolezza e la comprensione dei possibili problemi da parte di ciascuno.

L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) ha identificato per questi aspetti la necessità di promuovere una "cultura della sicurezza". Molti credono che l'utilizzo di misure quali firewall e software anti-virus impediscano del tutto le minacce alla sicurezza sia interne che esterne, tuttavia, l'efficacia delle tecnologie destinate a garantire la sicurezza dipende, in ultima analisi, dalla loro effettiva implementazione e dal comportamento di chi le implementa e le utilizza. La loro azione è resa più efficace fornendo agli utenti stessi le competenze e le conoscenze per riconoscere le minacce più comuni e intraprendere azioni preventive.

La crescita esponenziale di Internet e delle attività che ha generato, rende necessario lo sviluppo di comportamenti finalizzati alla sicurezza dell'operatività in rete. Certificare le competenze necessarie per identificare e affrontare minacce, quali il phishing e le transazioni fraudolente durante la navigazione sul Web e l'acquisto di beni e servizi online, può notevolmente migliorare la sicurezza online. L'utilizzo del social networking e dei social media sta diventando sempre più diffuso, sia per uso personale sia per lavoro; molti utenti, tuttavia, non sono a conoscenza di come entità terze possano accedere ad informazioni private che l'utente incautamente rende di dominio pubblico se non possiede le competenze e le conoscenze per impostare appropriati filtri, password e criteri di privacy.

La sicurezza di una rete si basa anche, come già detto in precedenza, sulle conoscenze e sul comportamento di ciascun individuo; per mantenere la sicurezza IT in un ambiente di rete, quale l'ambiente di lavoro, l'individuo deve prima possedere le competenze e le conoscenze per capire, ad esempio, le implicazioni di apertura di file sospetti, o le funzioni e limiti di un firewall. Un ulteriore elemento di sicurezza IT che viene spesso trascurato è quello della gestione sicura dei dati, sia per un individuo e per una organizzazione. Gestire i dati in modo sicuro copre una vasta gamma di procedure e attività, tra cui la necessità di effettuare periodicamente il backup memorizzando i dati in modo sicuro e la necessità di cancellare o distruggere permanentemente i dati sensibili che non si vuole che siano rintracciabili.

La sicurezza informatica, come si è evidenziato con queste brevi note, è un argomento di vasta portata, che tocca molti aspetti dell'attività individuale in ambito ICT. Attraverso questo modulo si vuole fornire al candidato le conoscenze e le competenze necessarie per identificare e trattare la maggior parte delle minacce associate all'uso delle tecnologie informatiche attraverso programmi mirati, arrivando a migliorare notevolmente le sue capacità di gestire in modo sicuro i propri dati ed i dati dell'organizzazione per cui lavora.

Lo Staff "AICA Digital Academy"

1 Concetti di sicurezza

1.1 MINACCE AI DATI

1.1.1 Distinguere tra dati e informazioni

Nel linguaggio di tutti i giorni, le parole *dato* e *informazione* hanno quasi lo stesso significato. In informatica, invece, è importante distinguerle:

- i **dati** sono numeri, testo o altro (ad esempio immagini) che si riferiscono a fatti non organizzati;
- le **informazioni** sono dati organizzati in modo da essere utili all'utente.

Un esempio servirà a essere più chiari: in una rubrica telefonica cartacea, costituiscono dei **dati** i nomi, i cognomi, gli indirizzi, i numeri di telefono che abbiamo annotato, mentre un nome collegato al proprio numero telefonico ed eventualmente anche all'indirizzo, rappresenta un'**informazione**.

Da questo esempio, si capisce che i dati, presi singolarmente, non hanno grande significato: a cosa servirebbero un paio di cognomi, un numero di telefono, qualche indirizzo, presi a caso, senza alcuna relazione tra loro? Se, invece, a un cognome corrisponde il proprio indirizzo e il proprio numero di telefono, allora abbiamo un'informazione che può esserci utile, perché, attraverso il cognome della persona possiamo risalire al suo indirizzo e ai suoi numeri di telefono.

I dati, quindi, **assumono significato quando sono organizzati tra loro in modo da costituire un'informazione.**

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

Quando un reato è commesso attraverso l'utilizzo di strumenti informatici, come il computer e Internet, è detto **crimine informatico**. Tra i più frequenti abbiamo:

- la copia non autorizzata di applicazioni o documenti (file musicali, video, ecc.) protetti dal diritto d'autore;
- l'accesso non autorizzato ai contenuti di un disco o di una banca dati;
- l'intercettazione di dati;
- il furto di identità;
- il phishing.

I metodi e le tecniche utilizzati per accedere illegalmente ai sistemi informatici altrui (perlopiù di enti o di grandi aziende) sono complessivamente definiti **hacking**; chi utilizza questi metodi e tecniche è detto **hacker**.

Il vero hacker è un profondo conoscitore dell'informatica, che non accetta le regole e gli interessi economici sempre più presenti nel mondo dei computer e di Internet. Quando riesce a entrare in un sistema protetto, non causa, in genere, danni, ma lascia un segno della sua visita, a volte comunicando il modo in cui è riuscito a superare i sistemi di sicurezza, così che l'azienda o l'ente possano evitare che questo riaccada in futuro.

In quest'ultimo caso si parla di **hacking etico**, così come quando sono le stesse aziende a commissionare l'uso di tecniche di hacking per testare la sicurezza dei propri sistemi e delle proprie reti.

Quando, invece, si accede a sistemi informatici altrui per rubarne i dati, trarne profitto o semplicemente per danneggiarli o distruggerli, si parla di **cracking** e chi lo pratica è detto **cracker**.

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

Altre minacce ai dati provengono da persone che hanno accesso ai dati informatici o alle stesse apparecchiature elettroniche e che possono danneggiarli o distruggerli (volontariamente in maniera dolosa, oppure involontariamente in maniera accidentale), oppure rubarli per utilizzarli a scopo personale o per rivenderli.

Queste persone possono essere gli impiegati della stessa azienda, personale che si occupa della manutenzione dei sistemi informatici, fornitori di servizi, oppure singoli individui od organizzazioni esterne che riescono ad accedere alla rete o direttamente ai dati.

In tutti i casi, è opportuno ricorrere all'utilizzo di account e password (limitano l'accesso ai dati alle sole persone autorizzate; ne parleremo nella Sezione 4 di questo Modulo), e a sistemi di protezione da intrusioni esterne, i cosiddetti firewall (ne parleremo nel punto 3.1.4).

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

I dati conservati nei sistemi informatici o utilizzati dai programmi non sono minacciati solo da persone malintenzionate, ma anche da eventi naturali (incendi, inondazioni, terremoti) o artificiali (guerre, rivolte popolari, fenomeni di vandalismo) in grado di danneggiare o distruggere sia i dati sia le apparecchiature.

Proprio per limitare questi **danni provocati da circostanze straordinarie**, è necessario effettuare una copia di sicurezza dei dati, da conservare in luoghi diversi da quelli dove i dati sono utilizzati (punti 7.1.2 e 7.1.3).

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

Il **cloud computing**, o più semplicemente **cloud**, è l'insieme di tecnologie che permettono l'accesso a risorse (applicazioni, memorizzazione online, altri servizi, ecc.) disponibili su Internet.

L'utilizzo del cloud è in crescente espansione, considerati i suoi numerosi vantaggi, tra cui la possibilità di accedere alle risorse ovunque sia possibile collegarsi alla rete, con un qualsiasi dispositivo; la condivisione di documenti e file con altri utenti, ecc.

Esistono, però, **minacce ai dati provocate dall'utilizzo del cloud**:

- l'eventualità che, a causa di accessi da parte di persone non autorizzate o dell'azione di malware (ad essi è dedicata la seconda Sezione di questo Modulo), avvengano **problemi che riguardano la protezione e il controllo dei dati**;
- **rischi per la privacy**: tutti i nostri dati sono registrati su memorie di massa di proprietà del provider. Inoltre, ogni volta che ci colleghiamo, sono trasmesse numerose informazioni: orario e durata del collegamento, da dove ci siamo collegati, che tipo di navigazione su Internet effettuiamo in quel momento, ecc.

1.2 VALORE DELLE INFORMAZIONI

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

Le tecniche per la sicurezza delle informazioni devono garantire tre caratteristiche fondamentali:

- **confidenzialità (o riservatezza)**: i dati devono essere accessibili solo a persone autorizzate, in nessun caso devono essere diffusi o visibili ad estranei;
- **integrità**: i dati devono essere modificati solo da persone autorizzate, in caso contrario il sistema deve segnalare eventuali modifiche non autorizzate o incompletezza dei dati;
- **disponibilità**: le persone autorizzate devono poter accedere ai dati protetti, il che significa che non devono essere richieste autorizzazioni o chiavi di accesso diverse da quelle in possesso degli utenti e che i dati vanno protetti con copie di sicurezza.

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

Quando le informazioni conservate in dispositivi elettronici riguardano una persona fisica (ad es. copie digitali di documenti, credenziali per accedere a una rete informatica, numeri di carte di credito, ecc.) sono dette **informazioni personali** e devono essere protette con particolare attenzione.

Infatti, malintenzionati possono appropriarsene al fine di utilizzarle per sottoscrivere un contratto, acquistare un prodotto, accedere a un servizio, fingendo di essere la persona alla quale appartengono le informazioni. In questi casi si parla di **frodi** e **furto di identità**, dei quali parleremo nella Sezione 1.3 (Sicurezza personale) di questo Modulo.

Il **diritto alla riservatezza** (comunemente definito col termine inglese **privacy**) è tutelato dalla legge anche per ciò che riguarda l'uso di sistemi informatici e Internet. Infatti, la diffusione di computer e Internet aumenta il rischio che informazioni personali da noi fornite a un'azienda o a un ente possano essere trasmesse ad altri. Attraverso il collegamento incrociato di banche dati, diviene così possibile ottenere un quadro piuttosto completo della personalità di un individuo, compresi aspetti riservati della sua vita: preferenze politiche, sessuali, stato di salute, condizioni economiche, ecc.

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

La maggior parte di uffici e aziende conserva, nei propri archivi digitali, **informazioni personali** dei propri clienti e impiegati e sono quindi obbligati per legge a tutelarle, per evitare che finiscano nelle mani di estraneo che potrebbero usarle per scopi illegali.

Nelle aziende, inoltre, sono a rischio di manomissione o furto anche le **informazioni commerciali o finanziarie** che riguardano direttamente l'azienda (ad es. progetti, investimenti, rapporti con banche ed enti, ecc.) e che potrebbero essere utilizzate o sabotate da aziende concorrenti.

Per tutti questi motivi, oltre che per il rischio di una perdita accidentale di dati, è indispensabile **proteggere le informazioni di lavoro memorizzate in computer e dispositivi mobili**.

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

Le **aziende** affidano a computer e reti interne un'enorme massa di dati, alcuni dei quali hanno particolare importanza per le aziende stesse, mentre altri riguardano informazioni personali relative a dipendenti e clienti.

Per questi motivi qualsiasi azienda, indipendentemente dalla sua dimensione, deve **gestire i problemi legati alla sicurezza dei dati trattati elettronicamente**, problemi che consistono principalmente nell'eventualità che persone non autorizzate possano accedere a quei dati e nella possibilità di perdita dei dati stessi, dovuta a disattenzione, malfunzionamenti, malware o altri motivi.

Tra le principali norme da seguire per evitare questi e altri simili rischi, c'è l'adozione di una politica di sicurezza nella **gestione dei cosiddetti "dati sensibili"**, attraverso la predisposizione di misure necessarie a impedire la perdita di questi dati (in seguito a eventi accidentali, furti, danneggiamento, distruzione) o la loro modifica (specie se si tratta di informazioni riservate). In tal senso sono indispensabili backup periodici dei dati (v. punto 7.1.3) e procedure di monitoraggio che permettano di risalire alle persone che hanno avuto accesso a dati riservati.

Inoltre, devono essere predisposte procedure per segnalare eventuali problemi di sicurezza, in modo che anche il solo sospetto di danni o di una diffusione impropria di informazioni riservate attivi immediatamente le necessarie contromisure. Infine, non va trascurata la preparazione dei dipendenti, che devono conoscere le proprie responsabilità riguardo alla sicurezza dei dati: ciò significa educarli a un uso accorto e riservato delle informazioni in loro possesso, a cominciare dall'utilizzo delle password d'accesso.

Nei paesi dell'Unione Europea, il **Regolamento Generale sulla Protezione dei Dati o GDPR del 2018** garantisce il *diritto alla privacy* e stabilisce che il trattamento dei dati personali debba rispettare tre principi:

- **trasparenza**: ogni persona ha diritto di essere informata quando i suoi dati personali sono elaborati elettronicamente;
- **scopi legittimi**: i dati personali possono essere elaborati solo per scopi dichiarati e legittimi;
- **proporzionalità**: il trattamento dei dati deve limitarsi a quanto strettamente necessario per gli scopi dichiarati, senza nessun eccesso.

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

In Italia, le norme che regolano l'utilizzo dei dati personali sono contenute nel Decreto Legislativo numero 196 dell'anno 2003, noto come "Testo unico sulla privacy", poi adeguato al **GDPR del 2018** di cui abbiamo parlato nel punto precedente.

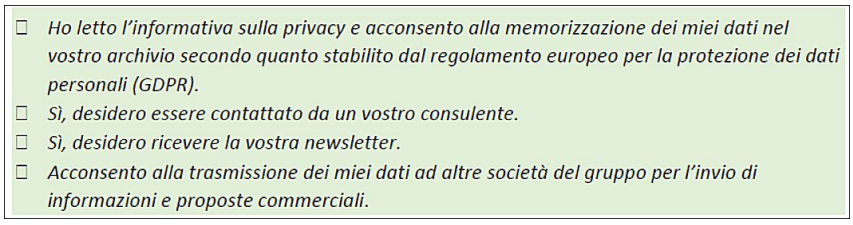
Punti essenziali di queste leggi sono:

- chi elabora dati personali è definito **controllore di dati**;
- le persone alle quali appartengono quei dati personali sono dette **soggetti dei dati**;
- nessuno può raccogliere e conservare dati personali altrui, senza il consenso scritto degli interessati;
- l'ente, la società, il professionista che conserva i dati deve nominare un responsabile del trattamento dati, che garantisca il rispetto delle leggi sulla privacy;
- le persone interessate possono chiedere informazioni riguardo il trattamento dei loro dati e, anche se hanno precedentemente dato il consenso alla loro elaborazione, possono chiedere la cancellazione dei dati, se ritengono violata la propria riservatezza;
- i dati personali devono essere cancellati appena cessa il motivo del loro utilizzo.

Se vengono raccolti dati senza il nostro consenso o utilizzati per scopi diversi da quelli permessi, il cittadino può ricorrere al **Garante della privacy** e, nel caso in cui venga attestato un danno morale o economico, ottenere anche un risarcimento.

Le aziende o gli enti che ci richiedono dati possono utilizzarli, ad esempio, per inviarci periodicamente delle notizie riguardanti le loro attività, per spedirci merce da noi richiesta, per trasmettere il nostro curriculum se siamo in cerca di lavoro. Non sono però autorizzati a utilizzare i nostri dati per scopi diversi da quelli che abbiamo accettato e devono adottare sistemi idonei a garantire sicurezza e segretezza dei nostri dati.

In genere, però, per risparmiare tempo, diamo il nostro consenso senza leggere con attenzione quanto ci viene chiesto di sottoscrivere; così capita molto frequentemente che senza accorgercene autorizziamo l'azienda alla quale comunichiamo i nostri dati a trasmetterli o rivenderli ad altre aziende. Ad es. nella fig. successiva l'unica autorizzazione indispensabile è la prima, ma la mancanza di indicazioni precise e la formulazione grafica ci spingono spesso a barrare tutte le caselle, concedendo così il nostro permesso a ricevere future proposte commerciali anche da parte di altre aziende sia tramite mail che telefonicamente (se abbiamo fornito un nostro recapito telefonico).


☐ *Ho letto l'informativa sulla privacy e acconsento alla memorizzazione dei miei dati nel vostro archivio secondo quanto stabilito dal regolamento europeo per la protezione dei dati personali (GDPR).*
☐ *Sì, desidero essere contattato da un vostro consulente.*
☐ *Sì, desidero ricevere la vostra newsletter.*
☐ *Acconsento alla trasmissione dei miei dati ad altre società del gruppo per l'invio di informazioni e proposte commerciali.*

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

Da tutto quanto abbiamo detto, è evidente che in ambito professionale e aziendale, quando si utilizzano strumenti informatici, **devono essere stabilite e rese note le norme che devono essere seguite da tutto il personale coinvolto**.

La scienza che si occupa di archiviare, elaborare, trasformare e trasmettere informazioni attraverso gli strumenti informatici è chiamata **ICT** (da "Information & Communication Technology").

A volte, il termine **ICT** è "italianizzato" in **TIC** (Tecnologie dell'Informazione e della Comunicazione) oppure abbreviato in **IT** ("Information Technology", in italiano "tecnologia dell'informazione").

Linee guida e politiche per l'uso dell'ICT sono stabilite, perciò, sia a livello generale che locale. A livello nazionale, è ad esempio possibile consultare il sito dell'*Agenzia per l'Italia Digitale* all'indirizzo web www.agid.gov.it. Se, invece, ci troviamo ad operare in una rete locale (come può essere quella di una scuola o di un'azienda), dovremo far riferimento all'amministratore di quella rete.

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

Con il termine **ingegneria sociale** (dall'inglese "social engineering") si indicano le tecniche utilizzate per accedere a informazioni riservate non eludendo protezioni hardware o software, ma **studiando il comportamento della persona che ha accesso a quel tipo di informazioni**, in modo che sia lei stessa a comunicarle, in maniera diretta o indiretta.

Un esempio per essere più chiari: il pirata informatico telefona a un impiegato di una società, spacciandosi per il gestore delle connessioni Internet e chiedendogli di fornire la password di accesso ad alcuni dati, in quanto è necessaria per risolvere un urgente problema di sicurezza. Di solito, il pirata informatico non telefona a una persona a caso, ma la sceglie sapendo che è in possesso dei dati che gli occorrono, che è più vulnerabile (ad esempio perché molto anziana, oppure poco esperta) e possiede già alcune informazioni che gli servono a confermare la sua falsa identità. Con i social network è ormai semplice acquisire questo tipo di informazioni: il pirata informatico può così telefonicamente rassicurare la persona con cui sta parlando, dicendogli di conoscere personalmente il direttore della società, la sua famiglia, alcuni avvenimenti personali e così via.

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

L'ingegneria sociale utilizza diversi metodi per rubare informazioni personali. Esaminiamo i principali.

Tra i sistemi più diffusi ci sono le **chiamate telefoniche**: spacciandosi per altre persone (come nell'esempio proposto al punto precedente) oppure fingendo di effettuare un sondaggio che permette di ottenere dei premi, il pirata informatico cerca di ottenere le informazioni che gli occorrono o, quantomeno, notizie che gli permetteranno di giungere successivamente, utilizzando altre tecniche, a quelle informazioni.

Il **phishing** si basa sull'invio di e-mail ingannevoli. Ad esempio, il pirata informatico invia un messaggio che apparentemente sembra provenire da una banca e che, minacciando la chiusura del conto o il blocco di una carta di credito, invita a collegarsi a una pagina web per inserire nome utente e password e confermare la propria identità. Se l'utente "abbocca all'amo" (questo è il significato letterale del termine "phishing"), le credenziali che digita saranno rubate dal pirata informatico e utilizzate per i suoi scopi.

Lo **shoulder surfing** consiste nel rubare le informazioni spiando direttamente la persona: ad esempio mentre digita la propria password al computer, oppure il PIN del bancomat o della carta di credito. L'osservazione può essere effettuata a occhio nudo (ad esempio stando alle spalle della persona, dal che deriva proprio il termine "shoulder surfing" che può essere tradotto con "spiare alle spalle") oppure tramite videocamere nascoste, cannocchiali o altro.

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

Quando il pirata informatico riesce ad acquisire una o più credenziali che permettono l'accesso a un servizio informatico (un singolo computer, una rete di computer, una casella di posta elettronica, un social network, un servizio bancario online, ecc.), avviene il cosiddetto **furto di identità**, in quanto il pirata può spacciarsi per la persona alla quale ha rubato i dati di accesso.

A quel punto, le **conseguenze** possono essere diverse:

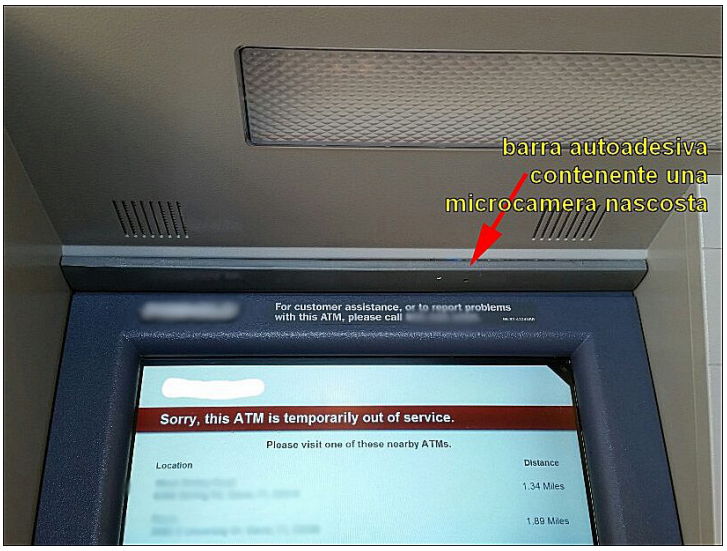
- **personali**: il pirata può inviare mail o scrivere messaggi nelle reti sociali e in entrambi i casi il tutto sembrerà essere opera della persona che è stata derubata delle sue credenziali di accesso;
- **finanziarie**: il pirata può acquistare prodotti online utilizzando la carta di credito del derubato;
- **lavorative**: queste pratiche possono danneggiare l'azienda per la quale lavora la persona derubata e possono condurre anche al licenziamento della persona stessa;
- **legali**: le azioni compiute dal pirata informatico appariranno effettuate dal derubato, che dovrà anche risponderne penalmente, cercando di dimostrare la sua innocenza.

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)

Per acquisire le informazioni necessarie a compiere un **furto di identità**, il pirata informatico utilizza diversi metodi, dei quali ricordiamo i principali:

- l'**information diving** consiste nel frugare tra oggetti e informazioni buttati via: nell'immondizia prodotta quotidianamente da un ufficio o da un ente sono spesso presenti foglietti, appunti, lettere, contenenti dati utili al pirata informatico. Ancora più ricchi di informazioni sono i vecchi computer buttati via da uffici o enti, dei quali i pirati informatici entrano in possesso a volte in maniera organizzata, ad esempio spacciandosi per volontari di società umanitarie che raccolgono vecchi computer per inviarli a paesi poveri. Anche se esistono modelli molto economici di macchine distruggi-documenti ed è abbastanza semplice estrarre un hard disk da un vecchio computer per distruggerlo, la maggioranza di uffici, aziende ed enti non utilizza queste cautele.

- Un metodo più tecnologico è lo **skimming** che ruba i dati incorporati in carte di credito, bancomat o badge, facendoli passare attraverso dispositivi fraudolenti di lettura o acquisendo i dati necessari attraverso l'utilizzo di fotografie e video, grazie ai costi e alle dimensioni ridotti e all'ottima risoluzione di fotocamere e videocamere digitali. Un esempio sono le microcamere nascoste da pirati informatici negli sportelli bancomat (fig. successiva): registrano i dati digitati dai diversi clienti che utilizzano lo sportello nella memoria della microcamera, che a fine giornata il pirata ritira e analizza.



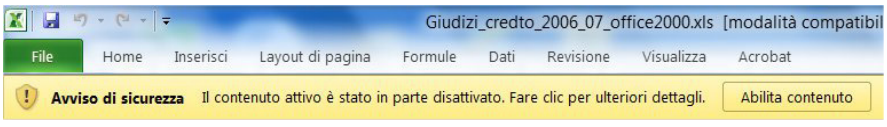
- Vi è poi il cosiddetto **pretexting**, che punta ad acquisire informazioni inventando uno scenario pretestuoso: ad esempio fingendo di essere un superiore, un collega di altro ufficio o filiale, telefonicamente – come nell'esempio del punto 1.3.1 – o tramite l'invio di mail, come nel caso del phishing.

1.4 SICUREZZA DEI FILE

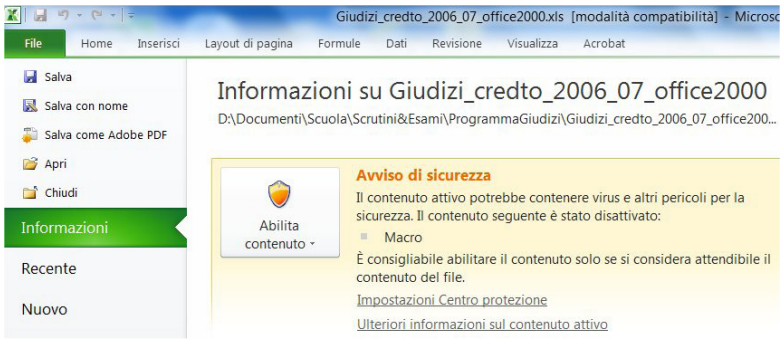
1.4.1 Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro

In diverse app di uso comune (*Word, Excel, PowerPoint*, ecc.) per effettuare alcune operazioni è necessaria una sequenza di comandi a volte lunga. Per questo motivo esistono le **macro**, che permettono, con un solo comando, di eseguire tutte le operazioni che si è provveduto a memorizzare. Ad esempio, con *Word* si può creare una macro che provveda con un unico comando a numerare tutte le pagine di un documento al quale stiamo lavorando, a crearne un sommario e ad effettuare il salvataggio del file.

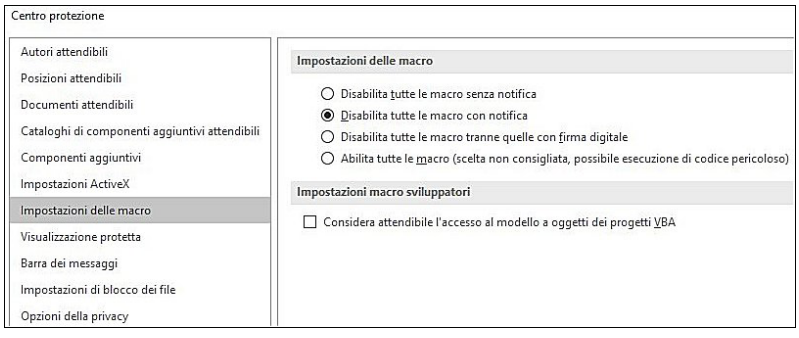
Essendo una specie di piccoli programmi, le macro, però, **possono nascondere al loro interno dei malware**. Per questo motivo, i programmi segnalano, al momento dell'apertura di un file, la presenza di una macro e chiedono l'autorizzazione ad eseguirla (fig. successiva).



Cliccando sulla scritta “Fare clic per ulteriori dettagli” si otterranno maggiori informazioni (fig. successiva). Se siamo sicuri della provenienza e dell’affidabilità del file, consentiremo l’esecuzione della macro. In caso contrario e se non è almeno possibile esaminare il file con un antivirus aggiornato, meglio disattivare le macro, anche se questo non consentirà di usufruire di tutte le possibilità offerte dal file.



È anche possibile modificare il modo in cui il programma gestisce le di macro, accedendo al *Centro protezione*. La procedura con i programmi del pacchetto *Microsoft Office* è la seguente: *File* > *Opzioni* > *Centro protezione* > *Impostazioni Centro protezione*. A quel punto – nella sezione *Impostazioni macro* – sarà possibile scegliere tra diverse opzioni (fig. successiva) che consentono di disattivare le macro con o senza notifica, di abilitare solo le macro fornite di firma digitale (e quindi provenienti da fonti che dovrebbero essere attendibili) oppure di eseguirle automaticamente senza nessun avviso (scelta molto rischiosa).



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

Per impedire accessi non autorizzati ai dati – siano essi propri o altrui, come nel caso delle aziende – è fondamentale utilizzare tecniche che, in caso di smarrimento o di furto, impediscano l’utilizzo del dispositivo (smartphone, tablet, portatile o altro) o del supporto di memoria (penna USB, scheda di memoria, disco rigido esterno) nel quale sono memorizzati questi dati.

Ciò è possibile, ad esempio, attraverso la **cifratura dei dati o crittografia**, che trasforma i dati in una serie di simboli incomprensibili a chi non possieda la “chiave” necessaria a renderli di nuovo utilizzabili.

Un file protetto con una password di apertura viene “cifrato”, vale a dire che un eventuale pirata informatico che ne entrasse in possesso e che cercasse comunque di aprirlo con altri programmi, si troverebbe di fronte una serie di simboli senza senso, in quanto non possiede la chiave di cifratura, vale a dire la password che abbiamo impostata.

Esistono comunque dei **limiti**:

- se dimentichiamo la password, la chiave o il certificato di cifratura non sarà possibile neppure a noi aprire il file;
- se scegliamo una password troppo semplice o prevedibile aumenta il rischio che un pirata informatico possa individuarla;
- vale la consueta raccomandazione di non divulgare per alcun motivo password, chiave o certificato di cifratura.

1.4.3 Cifrare un file, una cartella, una unità disco

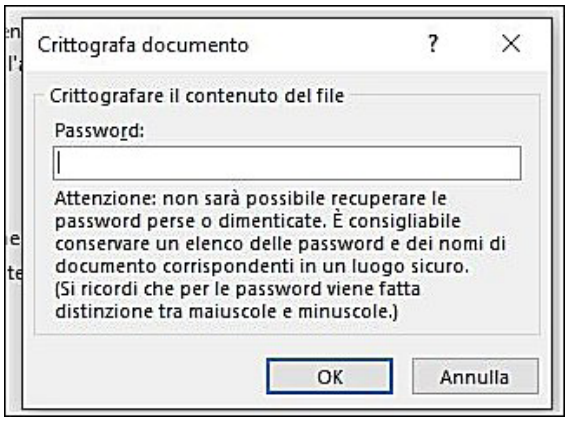
e

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

Un modo semplice e abbastanza sicuro per proteggere i nostri file di lavoro (documenti, fogli di calcolo, file compressi) da accessi non autorizzati è quello di **impostare una password per la loro apertura**. Vediamo le procedure necessarie.

Con *Word* occorre cliccare prima sulla scheda *File*, selezionare *Informazioni* nella colonna di sinistra e poi cliccare su *Proteggi documento* per accedere a diverse opzioni (fig. successiva);

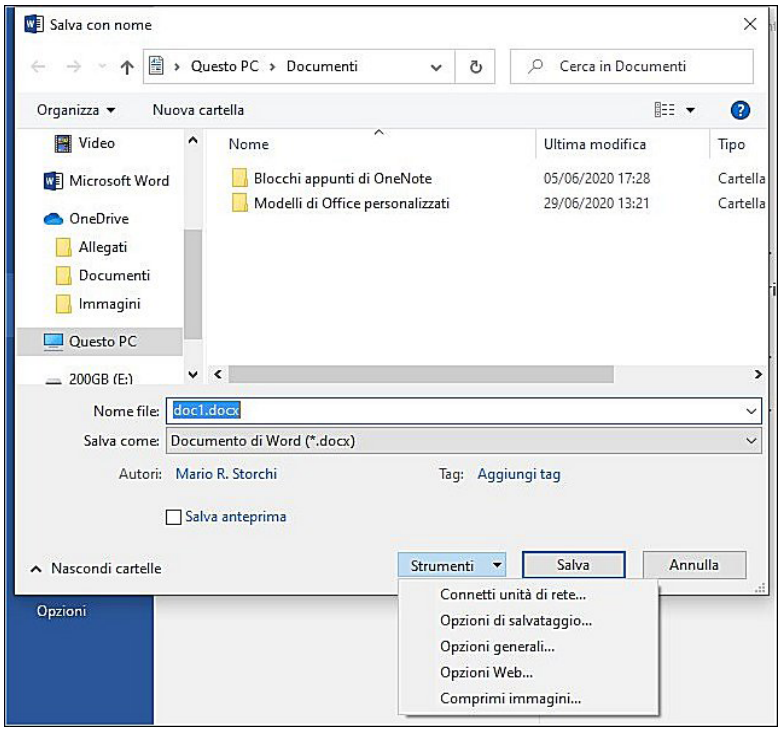
sceglieremo *Crittografa con password* per aprire la finestra *Crittografa documento* (fig. successiva), nella quale dovremo digitare la password che sarà necessaria per aprire il file. Il programma ci chiederà di digitare nuovamente la password (per evitare errori di battitura che renderebbero impossibile anche a noi l'accesso al documento), dopo di che per le successive aperture del file sarà richiesta la password.



Per eliminare la password di apertura basta ripetere l'operazione, stavolta lasciando vuota la casella dove andrebbe inserita la password.

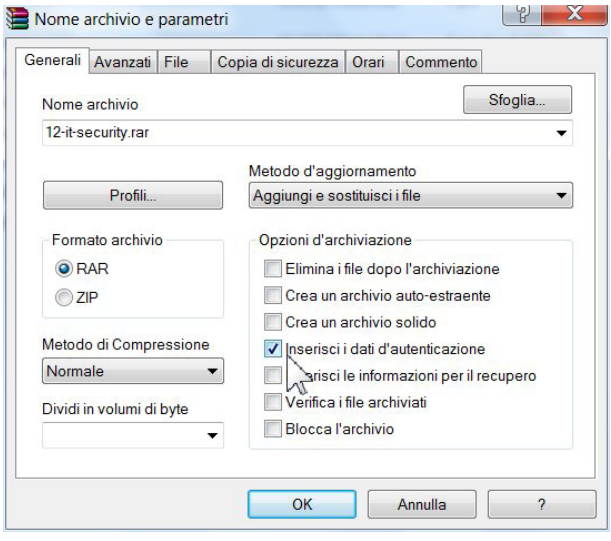
La procedura con *Excel* e altri programmi del pacchetto *Office* è simile, cambia solo qualche minimo particolare, ad esempio in *Excel* il pulsante *Proteggi documento* si chiama *Proteggi cartella di lavoro*.

Si può accedere all'impostazione della password di apertura anche in fase di salvataggio del file, ma la procedura è leggermente più laboriosa. Occorre scegliere prima su *Salva con nome*, poi – dopo aver scelto la posizione nella quale memorizzare il file – sul pulsante *Strumenti* che si trova in basso a destra e poi, dal menu a tendina che si apre, su *Opzioni generali* (fig. successiva). Nell'omonima finestra che si apre sarà possibile impostare la password di apertura.



È possibile **proteggere da aperture indesiderate** anche **i file compressi**, utilizzando uno dei programmi gratuiti di compressione come *WinRar* o *7Zip*, in quanto *Windows* permette di comprimere file ma non di proteggerli con una password.

I programmi di compressione, in genere, aggiungono delle voci di comando al menu contestuale che appare cliccando con il tasto destro su un file o su un gruppo di file. Con il programma *WinRar*, ad esempio, basta cliccare con il tasto destro sul file o sul gruppo di file e poi scegliere il comando *Aggiungi ad un archivio* per poi inserire il segno di spunta nella casella *Inserisci i dati d'autenticazione* (fig. successiva); una volta cliccato sul pulsante *OK* il programma ci chiederà di digitare la password. Con il programma *7Zip*, dopo aver scelto *Aggiungi* basterà digitare la password nel campo *Cifratura*.



Se si tratta di un file compresso già esistente, dovremo prima aprirlo col programma di compressione e poi scegliere l'opzione necessaria a inserire una password: in *WinRar* l'opzione è *File > Imposta parola chiave predefinita*, in *7Zip* occorre scegliere *Modifica password*.

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

Con il termine **malware** si indica ogni tipo di software creato per arrecare danni al contenuto di un dispositivo elettronico o all’attività di chi lo utilizza.

Poiché esistono molti tipi di malware, i danni da essi provocati sono estremamente diversi: da semplici fastidi come la comparsa di finestre pubblicitarie o rallentamenti del dispositivo, a veri e propri reati come la sottrazione di dati personali o il controllo a distanza del dispositivo infetto.

Nei punti immediatamente successivi illustreremo:

- le modalità con le quali vengono trasmessi i malware: trojan, rootkit, backdoor;
- i malware “infettivi”, che creano cioè copie di se stessi per diffondersi in altri dispositivi: virus e worm;
- i principali malware utilizzati per il furto di dati o altre truffe: adware, spyware, botnet, keylogger, dialer.

Vediamo quali sono i principali metodi con i quali si può nascondere il malware.

I **trojan** o **cavalli di Troia**, prendono questo nome perché la loro strategia assomiglia a quella utilizzata da Ulisse per penetrare con i suoi compagni nella città di Troia: nascosti all’interno di un enorme cavallo di legno che doveva sembrare un dono innocente. I trojan, infatti, contengono dei malware nascosti in programmi (ad esempio giochi), file video o audio, oppure sono allegati a mail apparentemente innocue. Una volta avviato il trojan, il malware si installa nel dispositivo e comincia a raccogliere informazioni riservate sulla persona che utilizza quel computer (password, altri codici come ad esempio quelli delle carte di credito utilizzate per acquisti via Internet) per poi inviare tramite Internet queste informazioni ai pirati informatici. Alcuni trojan permettono al pirata informatico di controllare via Internet il computer su cui è installato il virus, ovviamente solo quando questo computer è collegato in rete. A quel punto il malintenzionato può visionare l’intero contenuto del disco, copiarlo, modificarlo o cancellarlo a suo piacimento, in qualche caso addirittura controllare quanto succede nel locale dove si trova l’utilizzatore del dispositivo se a questo sono collegati e accesi un microfono o una web-cam.

I **rootkit** sono software che nascondono il funzionamento di altri programmi o processi, in modo che essi non vengano rilevati da antivirus o altri programmi di sicurezza. I rootkit, ad esempio, sono utilizzati per consentire il funzionamento di keylogger (punto 2.1.3) o di altri programmi spia e consentono al pirata informatico di controllare il sistema come se ne fosse il legittimo amministratore.

Le **backdoor** sono costituite da software che permette di accedere dall’esterno (tecnicamente si dice “da remoto”) a un sistema, aggirando l’inserimento di password o altre procedure di sicurezza. Alcuni malware, in particolare i trojan, creano delle backdoor per consentire l’accesso non autorizzato del pirata informatico al computer di un’altra persona.

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

Alcuni malware sono detti “infettivi” perché, una volta eseguiti, non agiscono solo sul dispositivo, ma **si moltiplicano**, creando copie di loro stessi che vengono inserite in programmi o inviate tramite posta elettronica.

Un **virus informatico**, ad esempio, è un piccolo programma creato per provocare danni ai computer e per diffondersi ad altri computer, così come i veri e propri virus, quelli biologici, si trasmettono da una persona a un'altra. Questo programma viene generalmente nascosto all'interno di altri file che possono essere anche allegati a una mail; quando utilizzate uno di questi file infetti, il virus si diffonde nel vostro computer e negli altri dispositivi eventualmente collegati in rete, andando a nascondersi in altri programmi. Esistono migliaia di virus, per cui i danni provocati vanno da rallentamenti o malfunzionamenti del computer sino a danni ai file o allo stesso sistema operativo, provocando anche il blocco del dispositivo.

I **worm** si diffondono attraverso la posta elettronica. Spesso, quando un computer viene contagiato da un worm, comincia a inviare automaticamente delle mail a tutti gli indirizzi presenti nella rubrica dei programmi adoperati per la posta elettronica, sfruttando i momenti nei quali un qualsiasi utente del computer infetto si collega a Internet e senza che la persona stessa se ne accorga. A ognuna di queste mail è allegata una copia dello stesso worm: la persona che riceve quel messaggio, rassicurata dal fatto che conosce il mittente, spesso apre l'allegato che contiene il malware e contagia il proprio computer. Attraverso questa continua moltiplicazione, il worm occupa uno spazio sempre maggiore nella memoria del computer, rallentandone le prestazioni, oltre ad altri problemi che può provocare.

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 sono creati per rubare i dati presenti in un dispositivo o in un sistema e poi trasmetterli all'esterno, alla persona che ha inserito il malware, nascondendolo in file scaricati da Internet. Vediamo quali sono i tipi più diffusi.

Gli **adware** sono un malware non particolarmente pericoloso, ma molto invadente: visualizzano sul dispositivo una serie continua di annunci pubblicitari, attraverso banner e popup. Oltre a rendere difficile la lettura delle pagine web, gli adware possono costituire anche un pericolo per la privacy, quando comunicano le nostre abitudini di navigazione a chi ha creato questo tipo di malware.

Il **ransomware** è un malware molto più dannoso, perché blocca il computer o ne cifra i contenuti, chiedendo il pagamento di una somma di denaro per sbloccare il dispositivo ("ransom" in inglese significa "riscatto").

Gli **spyware** sono piccoli programmi che si installano in maniera subdola nel nostro dispositivo e spiano tutte le nostre attività di navigazione su Internet. In pratica, trasmettono i dati della nostra navigazione a dei server remoti. Queste nostre preferenze saranno poi vendute a società commerciali che in base ai nostri gusti ci invieranno delle mail (il cosiddetto *spam*, del quale parleremo nel punto 6.1.3) o ci faranno apparire – mentre siamo collegati a Internet – delle finestre pubblicitarie collegate a siti che vendono materiale ritenuto di nostro interesse.

Con il termine **botnet** si indica una infezione che colpisce una intera rete informatica (come quella di una scuola, di un ufficio, di una azienda o di una rete dedicata allo scambio di file e programmi anche se protetti da diritto d'autore), in modo che il pirata informatico che l'ha diffusa riesce a prendere il controllo di tutti i dispositivi collegati a quella rete, senza il consenso dei rispettivi utenti.

I **keylogger** sono programmi che registrano tutti i caratteri digitati sulla tastiera (compresi dati privati come password, numeri di carte di credito, ecc.) per poi trasmetterlo a server remoti tramite Internet.

I **dialer** sono software inconsapevolmente scaricati da Internet, in genere cliccando su qualche link presente nel web o contenuto in una mail. Una volta avviato, il dialer interrompe il collegamento con il provider del cliente e collega il modem a un numero telefonico a tariffazione speciale (che di solito comincia con i numeri 199, 144, 899): così per scaricare una suoneria o un'immagine si spendono anche decine di euro. I dialer sono ormai poco diffusi, perché funzionano solo se la connessione a Internet avviene con la tradizionale linea telefonica, componendo un numero telefonico, mentre non hanno effetto con connessioni mobili, ADSL o fibra.

2.2 PROTEZIONE

2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta

Internet è il principale mezzo di trasmissione di virus, worm, cavalli di Troia, spyware e altri tipi di malware, perciò **è indispensabile utilizzare un software antivirus aggiornato**.

Un antivirus controlla i file contenuti nel nostro dispositivo e tutto ciò che in esso viene eseguito. Se, nel controllo, l'antivirus riconosce come sospetto un file, lo segnala all'utente e gli offre alcune opzioni:

- eliminare l'infezione dal file;
- eliminare il file;
- utilizzare il file, a proprio rischio;
- se un file risulta essere "sospetto" viene spostato in una cartella denominata "quarantena".

Windows 10 include già *Windows Defender Antivirus*; altri antivirus hanno costi contenuti o offrono versioni gratuite. È importante non far funzionare sullo stesso dispositivo più di un antivirus, altrimenti il dispositivo sarà rallentato e ognuno degli antivirus potrebbe segnalare come pericoloso l'altro software antivirus.

In ogni caso, occorre tenere presente che **nessun antivirus ci garantisce al 100%**, anche se installandone uno valido, aggiornandolo con regolarità e seguendo i consigli di sicurezza forniti in questo Modulo, è improbabile che il proprio dispositivo venga infettato.

Non tutti gli antivirus rilevano ed eliminano spyware e adware, in quanto non sono veri e propri virus. In questo caso è possibile scaricare, anche gratuitamente, applicazioni specifiche chiamate proprio *antispyware*. Un altro limite degli antivirus è la segnalazione di "falsi positivi", vale a dire file sicuri, che sono invece segnalati come contenenti virus.

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

Un software antivirus rappresenta, dunque, **una necessità non solo per i computer, ma per tutti i sistemi informatici che prevedono una connessione a Internet o ad altre reti**.

Come abbiamo detto, i sistemi operativi per computer dispongono in genere già di un proprio antivirus, ma esistono antivirus anche per dispositivi come tablet e smartphone che utilizzano altri tipi di sistemi operativi (*Android, IoS*, ecc.).

Un antivirus ben configurato e costantemente aggiornato, rende improbabile che un malware possa introdursi nel computer; è comunque consigliabile avviare di tanto in tanto manualmente la scansione del computer, oppure di file o cartelle sospette. Se sono presenti malware, l'antivirus ne indicherà il tipo e suggerirà la procedura da eseguire: se disinfettare, mettere in quarantena oppure eliminare il file.

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

Il mondo dell'informatica è in continua evoluzione, come dimostrano i nuovi software che sono quotidianamente realizzati. Il malware non fa eccezione a questa regola e anche di esso compaiono ogni giorno nuovi tipi, rapidamente distribuiti in tutto il mondo attraverso Internet.

Quando compare un nuovo malware, gli specialisti delle ditte produttrici di antivirus, sistemi operativi e applicazioni che possono essere contagiati, si mettono al lavoro e, in breve tempo, inseriscono nella banca dati le istruzioni per debellarlo.

Ovviamente, se non ci colleghiamo con il sito della casa produttrice (cosa che il sistema fa in genere da solo), il programma antivirus non potrà aggiornarsi e quindi non sarà in grado di riconoscere il nuovo malware e di impedirne l'ingresso nel computer o in altro dispositivo elettronico. L'unica cosa da fare, in questo caso, è anche la più semplice: **lasciare che il sistema proceda autonomamente a inserire gli aggiornamenti quando il dispositivo è connesso a Internet**, cosa che fa da solo senza disturbarci mentre navighiamo da un sito all'altro, se non per avvisarci della disponibilità degli aggiornamenti e della loro avvenuta installazione.

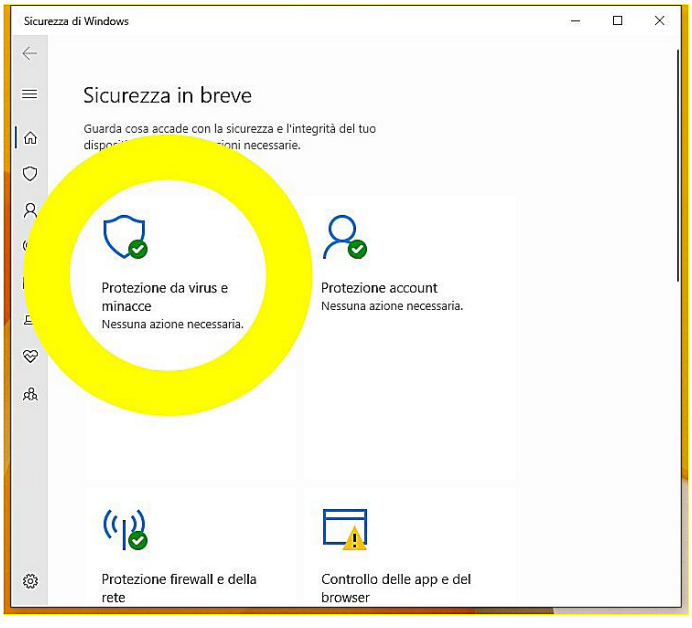
Gli aggiornamenti in genere avvengono automaticamente, ma a volte c'è un breve ritardo tra un nuovo virus che compare e l'aggiornamento che serve a segnalarlo e ad eliminarlo.

2.2.4 Eseguire scansioni di specifiche unità, cartelle, file usando un software anti-virus. Pianificare scansioni usando un software anti-virus

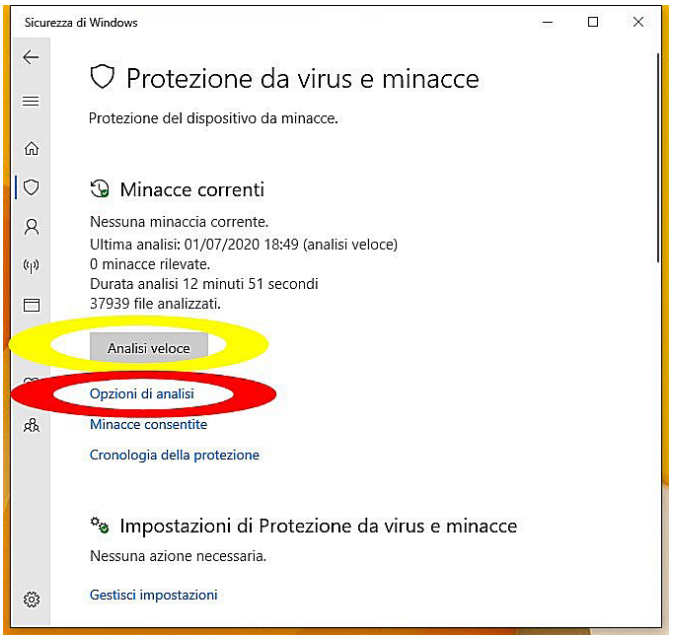
Il software anti-virus va automaticamente in funzione all'accensione del dispositivo nel quale è caricato e resta costantemente acceso, controllando tutti i file che vengono eseguiti, ma può anche essere utilizzato per eseguire la **scansione di specifiche unità, cartelle o file**, il che è utile per controllare file scaricati e allegati di posta elettronica prima di aprirli.

La scansione si attiva tramite l'interfaccia dell'antivirus, scegliendo tra le diverse opzioni cosa esaminare (unità, file, cartelle), quando e con che intervalli di tempo. Vediamo come effettuare queste operazioni utilizzando ***Defender,*** l'antivirus incluso in *Windows 10:*

1. apriamo l'app *Sicurezza di Windows* (la troviamo nell'elenco delle app; in alternativa possiamo scrivere nella casella di ricerca – accanto al pulsante *Start* – *Sicurezza* e poi scegliere *Sicurezza di Windows* dall'elenco dei risultati);



2. selezioniamo la prima opzione *Protezione da virus e minacce* (in giallo nella fig. successiva) per aprire l'omonima finestra (fig. successiva);

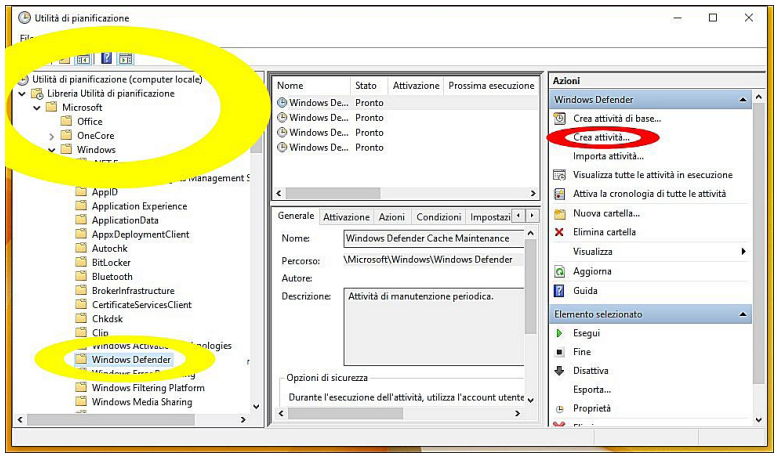


3. scegliamo *Analisi veloce* (in giallo nella fig. precedente) per controllare le cartelle in cui generalmente possono essere presenti minacce;
4. scegliendo *Opzioni di analisi* (in rosso nella fig. precedente) ci saranno offerte tre ulteriori opzioni:
   - *Analisi completa* controlla tutti i file presenti nel dispositivo: se sono particolarmente numerosi, l'analisi può richiedere oltre un'ora, ma possiamo continuare a utilizzare il dispositivo durante l'analisi;
   - *Analisi personalizzata* consente di scegliere file e percorsi da controllare;
   - *Analisi di Microsoft Defender Offline* serve a rimuovere software dannosi difficili da eliminare, tramite un riavvio del sistema e un controllo specifico (richiede mediamente un quarto d'ora).

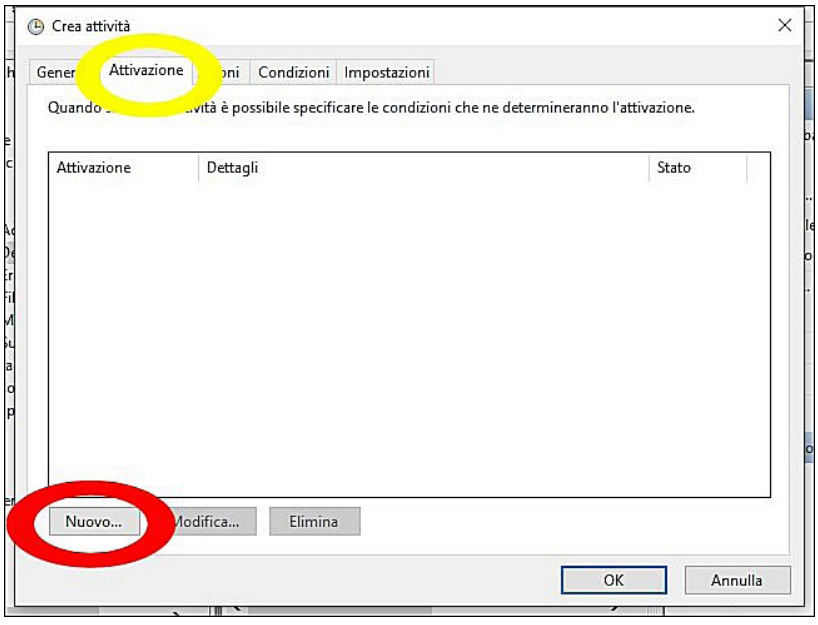
La **scansione** può anche essere **pianificata**, in modo che l'antivirus controlli, a intervalli definiti dall'utente, tutti o parte dei file contenuti nel dispositivo. Si può, ad esempio, scegliere di effettuare la scansione ogni settimana, in un giorno e orario in cui il computer è acceso ma poco utilizzato.

Per pianificare la scansione con *Defender* occorre utilizzare l'*Utilità di pianificazione*, seguendo questa procedura:

1. scriviamo nella casella di ricerca (accanto al pulsante *Start*), *pianifica* e scegliamo l'app *Utilità di pianificazione* dall'elenco dei risultati;
2. nella colonna di sinistra apriamo (cliccando sul cursore che si trova subito prima del nome) *Libreria Utilità di pianificazione* e quindi selezioniamo nell'ordine *Microsoft* > *Windows* > *Windows Defender* (in giallo nella fig. successiva);



3. nella colonna di destra clicchiamo su *Crea attività* (in rosso nella fig. precedente);
4. nell'omonima finestra che si apre clicchiamo prima sulla scheda *Attivazione* (in giallo nella fig. successiva) e poi sul pulsante *Nuovo* (in rosso nella fig. successiva);



5. a questo punto potremo scegliere quando dovrà essere avviato automaticamente *Defender* scegliendo tra le molte opzioni disponibili.

Chi usa *Linux* può utilizzare ***ClamAv***, che permette sia di scansionare file e cartelle, sia di pianificare scansioni scegliendo *Pianificatore* dal menu *Avanzate*.

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

Anche le app e i programmi informatici, il cosiddetto *software*, hanno un loro ciclo di vita e richiedono perciò un'azione periodica di verifica e manutenzione. Può infatti accadere che a un certo punto quei programmi e quelle app non siano più aggiornati dai produttori e non funzionino – in parte o del tutto – con sistemi operativi o hardware di nuova produzione.

Un software obsoleto e non supportato espone a diversi rischi:

- problemi di compatibilità con le applicazioni più recenti;
- lacune nella sicurezza che possono essere sfruttate dai criminali informatici per introdurre malware;
- rallentamenti dell'intera rete della quale fa eventualmente parte il dispositivo che utilizza quel software ormai superato.

In questi casi, è generalmente consigliabile cercare alternative convenienti e in grado di agevolare la propria attività.

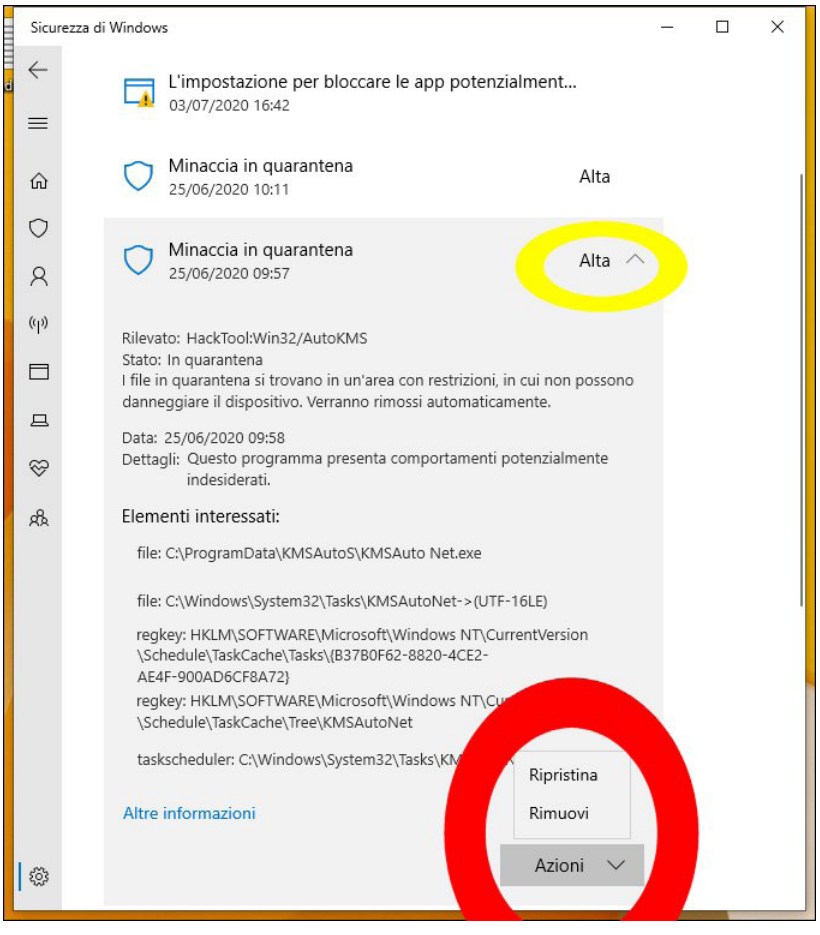
2.3 RISOLUZIONE E RIMOZIONE

2.3.1 Comprendere il termine "quarantena" e l'effetto di messa in quarantena file infetti/sospetti

Se l'antivirus individua dei file infetti o sospetti, ma non riesce a "disinfettarli" (vale a dire a ripulirli dal contenuto pericoloso), chiede all'utente se devono essere eliminati, oppure messi in **quarantena**, vale a dire spostati in un'apposita cartella creata dall'antivirus, nella quale i file resteranno ineseguibili sin quando un aggiornamento del programma antivirus permetterà di renderli nuovamente utilizzabili, oppure sin quando l'utente non deciderà di eseguirli (solo nel caso abbia la sicurezza assoluta che si tratti di una segnalazione errata) oppure di eliminarli definitivamente.

Gli antivirus permettono di scegliere se e in quali casi utilizzare la quarantena.

Ad esempio, con *Defender* dopo averlo avviato (*Sicurezza di Windows* > *Protezione da virus e minacce*): dovremo scegliere l'opzione *Cronologia della protezione* per aprire l'omonima finestra nella quale potremo vedere se ci sono file posti in quarantena e decidere se rimuoverli oppure ripristinarli aprendo il relativo menu selezionando prima il pulsante evidenziato in giallo nella fig. successiva e poi quello evidenziato in rosso. Se decidiamo per il ripristino, dovremo essere assolutamente certi che non contengano malware, altrimenti rischieremmo di infettare tutto il dispositivo.



2.3.2 Mettere in quarantena, eliminare file infetti/sospetti

Se sono presenti malware, l'antivirus ne indicherà il tipo e suggerirà la procedura da eseguire: se disinfettare, mettere in quarantena oppure eliminare il file. Queste opzioni dipendono dal tipo di malware:

- *Disinfetta*: l'antivirus è in grado di eliminare il malware dal file infetto e restituirci il file com'era prima dell'infezione.

- *Metti in quarantena:* l'antivirus non è in grado di disinfettare il file contagiato, lo posiziona quindi in una cartella protetta in attesa di scaricare dalla casa produttrice dell'antivirus un aggiornamento che permetta di eliminare quel tipo di malware.
- *Elimina:* il programma non è in grado di svolgere le prime due operazioni e quindi l'unica soluzione è l'eliminazione del file.

Quest'ultima opzione riguarda spesso i CD e i DVD, sui quali il programma non può intervenire giacché, una volta inciso, il dischetto a lettura ottica non è modificabile. Non essendo possibile eliminare il file da un CD o DVD, i supporti risultano inservibili (a meno di voler infettare il computer nel quale verranno utilizzati).

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

Contro il malware, a parte la prudenza e i software antivirus (che costituiscono i due elementi più importanti), è possibile **adoperare anche risorse online**.

I **siti web di software antivirus** spesso mettono gratuitamente a disposizione degli "scanner on line" che consentono di diagnosticare la presenza di malware. Meno frequente, purtroppo, la possibilità che questi scanner eliminino il malware, in quanto come soluzione viene generalmente proposto l'acquisto o almeno l'installazione in periodo di prova del software antivirus.

Utile risulta anche la consultazione periodica di **siti di sistemi operativi, browser web, autorità preposte** (ad es. la Polizia di Stato) che aggiornano spesso sulle minacce malware più diffuse e pericolose, a volte rendendo possibile lo scaricamento gratuito di tool di rimozione del codice pericoloso.

Proprio per questo motivo, i malware più pericolosi impediscono la connessione a Internet dei dispositivi che colpiscono. In questi casi è ovviamente possibile utilizzare un altro dispositivo per accedere alle risorse online di cui sopra.

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)

In informatica, il termine **rete** indica un sistema di collegamento tra due o più computer o dispositivi elettronici di altro tipo (tablet, smartphone, ecc.), dotati di una apposita scheda di rete e del relativo software di collegamento, che permette alle persone che utilizzano uno qualsiasi di quei dispositivi di sfruttare non solo le risorse del proprio apparecchio (vale a dire le applicazioni e i dati presenti su esso), ma anche quelle condivise degli altri computer, dispositivi ed eventuali periferiche (ad esempio stampanti o unità di memoria) collegate in rete.

Per fare un esempio: se nel computer di un amico è presente un documento e il mio tablet è collegato alla stessa rete di quel computer, in assenza di eventuali restrizioni poste dal mio amico, posso visualizzare quel documento, anche se materialmente esso non è presente nel mio dispositivo.

Così come è possibile collegare due dispositivi, è possibile collegarne dieci, cento o mille: in ogni caso quella che si realizza è sempre una rete, in inglese **network**, o, più brevemente, **net**.

In base alla loro estensione, le reti si dividono principalmente in:

Reti locali o LAN: limitate a un’area circoscritta (una scuola, un ufficio, un’azienda), in genere non più ampia di 10 km. In una rete LAN esiste di solito un computer principale e più potente, detto **server**, che mette le proprie risorse a disposizione degli altri elaboratori della rete, chiamati **client**. Dal momento che i dispositivi sono collegati attraverso l’utilizzo dei cavi, la rete è detta **cablata** e di solito garantisce una maggiore sicurezza, in quanto i dispositivi sono collegati in modo fisico e quindi visibile. Inoltre, i cavi assicurano in genere velocità di scambio dei dati maggiori rispetto alle onde radio.

Se la rete non utilizza i fili per collegare i vari dispositivi, ma le onde radio, si aggiunge il prefisso “W” (da “Wireless”) ed è quindi detta **WLAN o rete locale wireless**. Le **reti wireless** sono più economiche e semplici da installare, non richiedendo la posa di cavi. Se poi non è materialmente possibile far arrivare un cavo per collegare un dispositivo, il wireless è l’unica soluzione possibile. In genere, le WLAN sono protette da una password che impedisce l’accesso alle persone non autorizzate per garantire un accesso sicuro a dati e risorse. In alcuni luoghi pubblici (bar, hotel, locali commerciali, aeroporti, ecc.) esistono WLAN alle quali è possibile accedere liberamente.

Reti geografiche o WAN: collegano tra loro computer distanti tra loro, oppure reti locali, coprendo, quindi, vaste aree. Anche Internet può essere considerata una WAN, per la precisione la più estesa di tutte le WAN.

VPN (da “Virtual Private Network”): utilizzano Internet (vale a dire una rete pubblica) per creare delle reti private (il cui accesso è quindi consentito solo a persone autorizzate) che collegano computer e dispositivi lontani tra loro. Attraverso una VPN, ad esempio, le aziende creano proprie linee private tra le diverse sedi, in modo da poter sfruttare in sicurezza tutti i servizi dell’azienda. La VPN utilizza un’autentificazione per garantire l’accesso ai soli utenti autorizzati e tecniche di crittografia per evitare il furto di dati.

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

La connessione in rete – in particolar modo alla più grande di queste reti: Internet – **offre vantaggi spesso irrinunciabili**: basti pensare all’utilizzo molto limitato che si potrebbe fare di uno smartphone o di un tablet non collegati a Internet.

D'altra parte, **la connessione a una rete** – sia essa una rete locale, come quella presente in molte scuole, uffici o aziende, oppure Internet – **comporta minacce alla sicurezza dei dati**. Le principali implicazioni di sicurezza sono:

- **trasmissione di malware**, che possono essere contenuti in allegati di posta elettronica, pagine web, programmi o altro;
- **accessi non autorizzati** ai dispositivi collegati e, conseguentemente, a tutti i dati in essi contenuti, a causa di difetti nella sicurezza o infezioni virali;
- **pericoli per la privacy**, sia perché in caso di accessi non autorizzati sono a rischio tutti i dati personali contenuti nei dispositivi collegati in rete, sia perché tutte le operazioni compiute all'interno della rete sono monitorate per ragioni di sicurezza (un amministratore di rete è in grado, ad esempio, di conoscere quando un utente si è collegato alla rete e quali siti ha visitato).

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

Ogni rete viene gestita da un **amministratore di rete**, che ha la possibilità di effettuare interventi non consentiti agli altri utenti; ad esempio:

- **assegnazione** degli account (necessari per accedere alla rete) ai singoli utenti o a singoli dispositivi;
- **autorizzazione** degli account, assicurandosi che possano collegarsi senza problemi alla rete e stabilendo per ogni account i cosiddetti "privilegi", vale a dire quali operazioni sono permesse e quali vietate;
- **autenticazione** degli ingressi, attraverso password o altre procedure (schede magnetiche, impronte digitali, ecc.) che accertino l'identità di chi vuole accedere alla rete.

Inoltre, l'amministratore di rete ha il compito di controllare la sicurezza del sistema, attraverso le seguenti operazioni:

- **verifica e installazione di patch e aggiornamenti di sicurezza importanti**;
- **controllo del traffico di rete**;
- **trattamento dell'eventuale malware rilevato in rete** al fine di disinfettare, porre in quarantena o eliminare i file pericolosi (come spiegato ai punti 2.3.1 e 2.3.2).

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

Un virus informatico si riproduce nel computer infettando i file e utilizzandoli come mezzo di trasmissione (essendo nascosto al loro interno), per cui può essere bloccato da un antivirus aggiornato. Altri tipi di malware, invece, infettano i computer utilizzando i mezzi di comunicazione tra i dispositivi elettronici (innanzitutto Internet e la posta elettronica) e infiltrandosi come componenti del sistema operativo: per bloccarli non è quindi sempre sufficiente un antivirus, ma occorre un firewall.

Il **firewall** è un sistema di sicurezza che determina quali dati possono passare da Internet al dispositivo collegato in quel momento alla rete e viceversa, in modo da cercare di evitare che estranei possano accedere a dati presenti in un computer collegato a Internet, o trasmettere malware.

Il firewall può essere costituito sia da un software (quasi tutti i sistemi operativi comprendono già al loro interno un firewall) sia da un apparato (ad esempio molti modem-router che servono a collegarsi a Internet dispongono di un firewall) o da un altro PC usato per questa funzione.

Il firewall segnala sia quando un programma contenuto nel dispositivo cerca per la prima volta di accedere a Internet, sia eventuali tentativi di intrusione dall'esterno, impedendo che il computer risponda alle istruzioni esterne.

In questi casi, il firewall propone in genere **quattro tipi di scelta**:

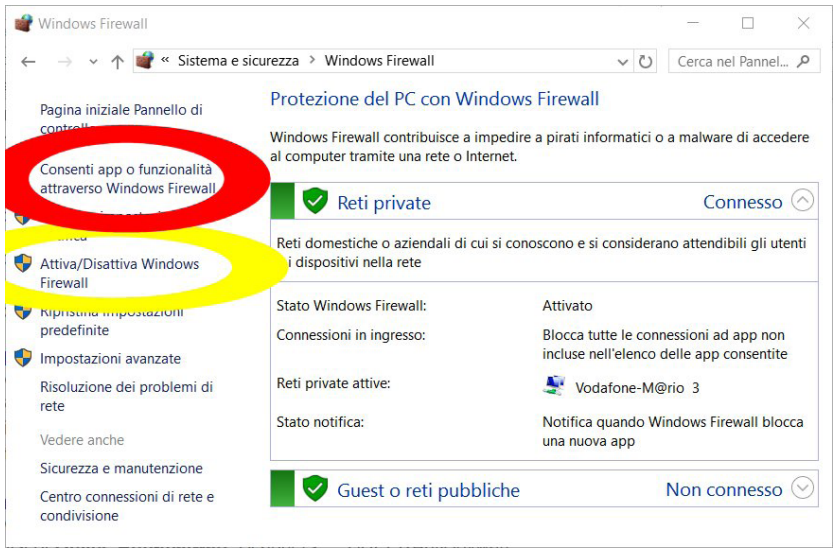
- *Sì, solo per questa volta* (viene permesso lo scambio di dati, ma la volta successiva verrà riproposta la domanda);
- *Sì, sempre* (sarà sempre consentito quel tipo di scambio di dati);
- *No, solo per questa volta* (viene impedito lo scambio di dati, ma la volta successiva sarà riproposta la domanda);
- *No, sempre* (quel tipo di scambio di dati sarà sempre impedito).

Una cattiva configurazione del firewall è il principale motivo dei suoi limiti: se, ad esempio, l'amministratore della rete blocca tramite il file delle connessioni necessarie a determinati programmi o funzioni, essi non potranno essere utilizzati pienamente. Al contrario, se consente connessioni non necessarie, queste potrebbero essere sfruttate da malintenzionati per accedere alla rete. Inoltre, un firewall non rileva la presenza di virus nei dati trasmessi e ricevuti ed è ovviamente impotente in caso di errori del personale interno o di uso di tecniche di "ingegneria sociale" (punto 1.3.1).

In linea generale, è consigliabile autorizzare solamente l'indispensabile: se non siete sicuri di cosa fa un certo programma che chiede l'autorizzazione, non autorizzatelo; acconsentite solo se l'uso di Internet è impossibile senza quest'autorizzazione.

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

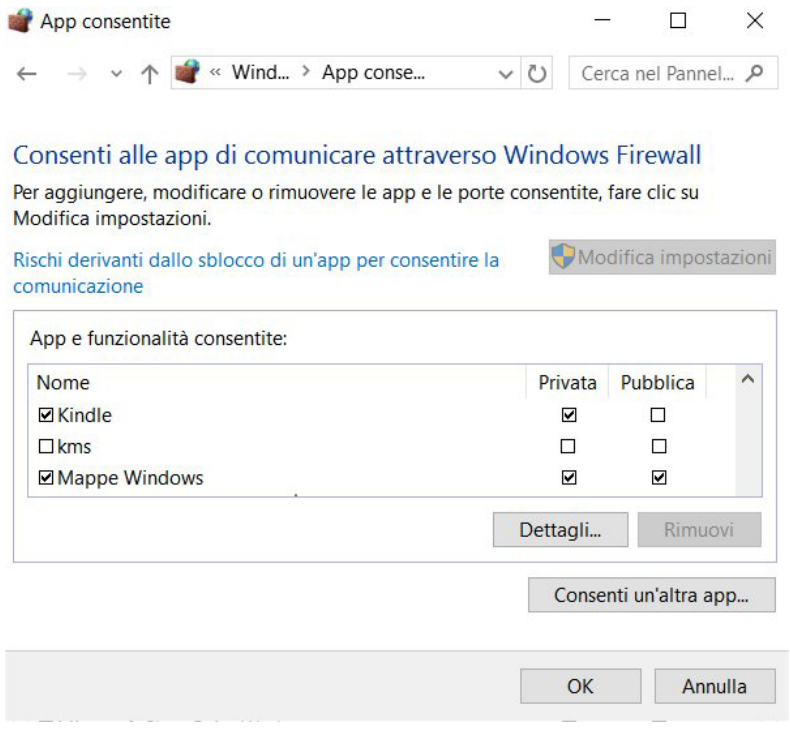
Windows 10 dispone di *Windows Defender Firewall.* Per accedere alle sue impostazioni cominciamo a digitare *firewall* nella casella di ricerca e poi scegliamo *Windows Defender Firewall* dall'elenco dei risultati. In alternativa possiamo scegliere dall'elenco delle app *Sistema Windows* > *Pannello di controllo* > *Sistema e sicurezza* > *Windows Defender Firewall.*



Nell'omonima finestra che si apre (fig. precedente) troviamo a sinistra una colonna contenente diverse opzioni tra cui:

- ***Attiva/Disattiva Windows Firewall*** per abilitare o disabilitare il servizio (potrebbe esserci richiesto di immettere una password amministrativa o di confermare la scelta);

- ***Consenti app o funzionalità attraverso Windows Firewall*** apre un'ulteriore finestra nella quale potremo consentire o bloccare la connessione ad applicazioni, servizi o funzioni inserendo o disinserendo il segno di spunta nelle relative caselle (potrebbe esserci richiesta una password amministrativa o comparire un riquadro nel quale confermare la scelta). Nella fig. successiva, ad esempio è consentita la connessione all'app *Kindle* solo quando siamo collegati in una rete privata (ad es. a casa), mentre è vietata se stiamo utilizzando una rete pubblica (ad es. quella messa gratuitamente a disposizione in alcuni esercizi commerciali o stazioni); è inoltre vietata ogni connessione al servizio denominato *kms* mentre sono consentite le connessioni sia su rete privata che su rete pubblica per il servizio *Mappe di Windows*.



Le operazioni sono generalmente simili anche se utilizziamo altri firewall personali.

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 garantire la sicurezza delle reti wireless si utilizzano sistemi di cifratura dei dati (della cifratura abbiamo parlato al punto 1.4.2), in modo che eventuali malintenzionati che riuscissero a intercettare i dati non sarebbero comunque in grado di leggerli.

Il primo sistema di cifratura ad avere grande diffusione è stato il **WEP**, oggi però sostituito dal più affidabile **WPA**, del quale esiste anche una versione **WPA2** che rende ancora più efficace la protezione dei dati inviati e ricevuti.

Per ulteriore sicurezza, può essere utilizzato anche il cosiddetto **MAC** o **MAC address**, che consiste in un indirizzo scritto in linguaggio esadecimale (vale a dire suddiviso in 6 coppie di cifre; ad es.: 00:1F:3B:3C:5F:2F), che identifica ogni scheda di rete. Il MAC è impostato di fabbrica e quindi, per una ulteriore sicurezza nelle reti wireless, può essere creata una lista degli indirizzi MAC dei dispositivi autorizzati a utilizzare quella rete. Un estraneo, anche se a conoscenza della password di accesso, non potrebbe accedere alla rete, in quanto non verrebbe riconosciuto come valido l'indirizzo MAC del dispositivo che sta utilizzando. Va comunque tenuto presente che esistono sistemi che consentono a persone esperte di falsificare il MAC di una scheda di rete.

È anche possibile nascondere il **nome della propria rete o SSID** (da "Service Set Identifier") in modo che essa non compaia a estranei nell'elenco delle reti disponibili a cui connettersi. Anche in questo caso si tratta di un metodo aggirabile, in quanto alla persona estranea basta conoscere il nome della rete per effettuare la connessione.

Non esiste, quindi, un metodo in grado di garantire totalmente la sicurezza di una rete wireless, ma la conoscenza dei diversi metodi e il loro utilizzo – soprattutto in maniera combinata (ad esempio una chiave WPA2 unita a una lista di indirizzi MAC) – assicura un elevato 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 wireless non è protetta con i metodi indicati al punto precedente, è semplice per un estraneo accedervi o solo per utilizzare gratuitamente la connessione a Internet, oppure per accedere ai dati presenti nei dispositivi e scambiati in rete. Il rischio non è solo del proprietario della rete, ma anche di chi si collega a essa senza averne l'autorizzazione, in quanto anche i suoi dati vengono scambiati senza cifratura.

I **principali attacchi ai quali si va incontro usando una rete wireless non protetta** sono effettuati da:

- **intercettatori o "eavesdropping"** che intercettano i dati scambiati in rete. Alcuni pirati informatici, ad esempio, creano volutamente reti wireless non protette, in modo da poter intercettare i dati di chi si collega a esse, convinto di essere stato fortunato a trovare una rete aperta con la quale collegarsi gratuitamente a Internet.
- **dirottatori di rete o "network hijacking"** che reindirizzano la nostra navigazione verso annunci pubblicitari e siti carichi di spyware e virus.
- **violatori di comunicazioni private o "man in the middle"** che sono in grado di leggere, inserire o modificare messaggi tra due persone che stanno avendo una conversazione privata in rete attraverso un social network, una chat o altro.

3.2.3 Comprendere il termine "hotspot personale"

In informatica, il termine hotspot indica un luogo in cui è presente una connessione a Internet pubblica: esercizi commerciali, stazioni, ecc. nei quali il collegamento a Internet è aperto a chi si trova in quei luoghi.

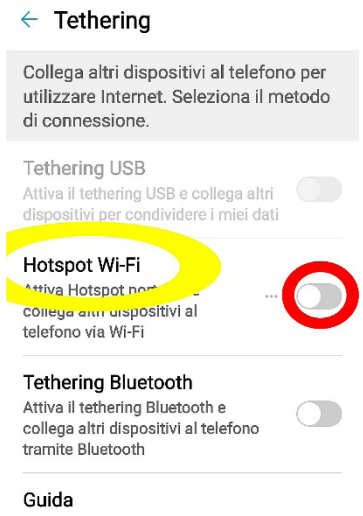
Il termine **hotspot personale** indica, invece, la condivisione di un collegamento a Internet attraverso un dispositivo personale, utilizzando la funzione wireless.

L'esempio più frequente è quello di uno smartphone nel quale è inserita una SIM che permette una connessione dati. Il proprietario dello smartphone può utilizzare il suo dispositivo come punto di accesso dotato di collegamento web cui possono collegarsi computer, cellulari e tablet. Si tratta di una tecnica sempre più utilizzata, specie quando la SIM dello smartphone permette una connessione a prezzi contenuti, come nel caso di piani telefonici che prevedono a fronte di un canone mensile contenuto uno scambio dati di alcuni gigabyte.

3.2.4 Abilitare, disabilitare un hotspot personale e connettere, disconnettere dispositivi in modo sicuro

Vediamo, nella pratica, come **abilitare un hotspot personale con un dispositivo funzionante con il sistema operativo *Android***. Le istruzioni si riferiscono alla versione 9 di *Android*, ma sono simili anche per altre versioni.

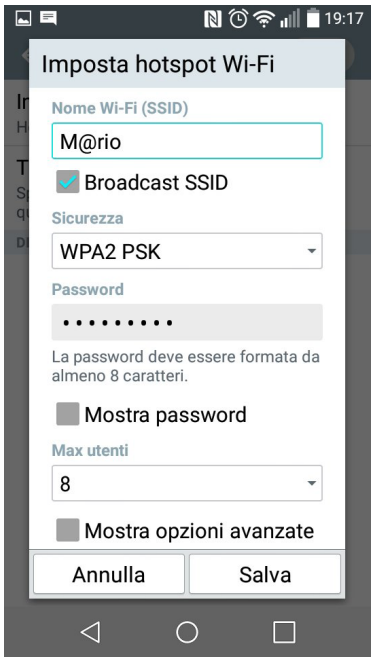
Apriamo il menu *Impostazioni*. Sotto la voce *Rete* scegliamo prima *Tethering* e poi *Hotspot Wi-Fi* facendo attenzione a toccare la scritta (evidenziata in giallo nella fig. successiva) e non il pulsante di attivazione/disattivazione del servizio (evidenziato in rosso).



Nella nuova finestra che si apre dovremo cliccare su *Imposta hotspot Wi-Fi* per impostare i dati di accesso (fig. successiva):

- il *nome della rete Wi-Fi o SSID*, per il quale potremo accettare quello proposto o digitarne uno di nostro gradimento;
- il tipo di *sicurezza* da utilizzare per la connessione: possiamo generalmente scegliere tra *aperta* a tutti (che non necessita di alcuna password, un'opzione da evitare); *WPA PSK*; *WPA2 PSK*;
- la *password* che dovrà essere digitata per collegarsi all'hotspot personale.

Dopo aver effettuato le nostre scelte, confermiamo scegliendo *Salva*.



A questo punto l'hotspot personale è stato configurato e deve essere abilitato. Torniamo perciò al menu *Tethering & Reti* e attiviamo l'*Hotspot Wi-Fi* toccando, stavolta, il pulsante di attivazione/disattivazione del servizio e non la scritta.

L'hotspot è ora in funzione. Per **connettere a esso un dispositivo** (ad esempio un tablet o un altro smartphone privi di collegamento a Internet) basterà aprire il menu Wi-Fi del dispositivo da collegare, trovare la nuova rete wireless che abbiamo creato, selezionarla e inserire la password.

Praticamente le stesse procedure servono a **disabilitare l'hotspot** (*Impostazioni* > *Rete* > *Tethering* > *Hotspot Wi-Fi* > toccare il pulsante per disattivare il servizio) e a **disconnettere il dispositivo** (*Impostazioni* > *Wi-Fi* > selezioniamo il nome dell'hotspot personale > *Elimina rete*).

Per **abilitare un hotspot personale con iPhone** dovremo:

- accedere alle *Impostazioni di iOS* pigiando sull'apposito pulsante presente nella schermata principale;
- selezionare la voce *Cellulare*;
- accertarci che le opzioni *Dati cellulare* e *Abilita 4G* siano attivate;
- scorrere la schermata e pigiare su *Hotspot personale* per accedere alle impostazioni della funzione di hotspot (fig. successiva);
- impostare una password rete pigiando sulla voce *Password Wi-Fi*;
- spostare su *ON* la levetta dell'opzione *Hotspot personale*.

Anche nel caso dell'iPhone, dopo aver attivato l'hotspot personale possiamo collegarci a esso da qualsiasi tablet, smartphone, computer o altro dispositivo dotato di funzione Wi-Fi (indipendentemente dal sistema operativo che utilizza) usando la procedura spiegata sopra.

Per **disattivare l'hotspot personale di iPhone** basta spostare su *OFF* la levetta dell'opzione *Hotspot personale* (fig. precedente).

4 Controllo di accesso

4.1 METODI

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

Esistono diversi **metodi per impedire accessi non autorizzati ai dati** che utilizziamo, in modo particolare quando i rischi sono più elevati, ad esempio quando i dati da proteggere sono memorizzati su dispositivi mobili, oppure quando utilizziamo una connessione senza fili.

Identifichiamo i metodi di protezione più comuni ed efficaci:

- l'identificazione all'accesso tramite la digitazione di **nome utente e password**, che è il sistema più utilizzato per l'accesso a computer e siti web;
- l'utilizzo di un **PIN** (dalle iniziali di "Personal Identification Number", sign. "numero di identificazione personale"), vale a dire un codice numerico (in alcuni casi sostituito da un segno grafico o dall'impronta digitale) che può ad esempio essere richiesto al momento dell'accensione del proprio dispositivo mobile, per impedire che altre persone possano utilizzarlo, specie in caso di smarrimento o di furto;
- la **cifratura dei dati**, che abbiamo trattato nei punti 1.4.2, 1.4.3 e 1.4.4;
- l'**autenticazione a più fattori**, che consiste nell'associare un qualcosa che si conosce (ad es. una password o un PIN) a un qualcosa che si ha con sé (ad es. un oggetto fisico come lo smartphone o una tessera magnetica). Anche le carte Bancomat utilizzano questo tipo di autenticazione a più fattori, in quanto per accedere al servizio occorre conoscere il PIN e avere con sé la tessera. In campo informatico l'autenticazione a più fattori è utilizzata da diversi servizi in rete che permettono l'accesso dopo l'inserimento non solo di nome utente e password, ma anche di un codice inviato tramite un messaggio al telefonino dell'utente.

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

Per proteggere l'accesso ai dati, può essere utilizzata anche la **one-time password**, vale a dire una password valida una sola volta. In questo modo, anche se altre persone venissero a conoscenza di questa password, essa risulterebbe inutile, in quanto valida per una singola operazione e in genere con una durata limitata a qualche minuto.

Per ulteriore sicurezza, la one-time password è di solito trasmessa all'utente attraverso un canale differente da quello utilizzato per la trasmissione dei dati, utilizzando una autenticazione a più fattori come quella spiegata nel punto precedente. Ad es. nel caso di diversi servizi bancari, se siamo collegati attraverso un computer, essa ci può essere inviata tramite SMS, posta elettronica, oppure comparire su un apposito dispositivo (fig. successiva) o, più spesso, in una app per smartphone, forniti dalle banche ai propri clienti.

4.1.3 Comprendere lo scopo di un account di rete

Lo **scopo di un account di rete** è duplice:

- autenticare l'identità di un utente attraverso l'inserimento di una password associata all'identificativo dell'utente;
- autorizzare (o negare) l'accesso alle risorse di dominio in base alle autorizzazioni assegnate a quell'utente per le specifiche risorse.

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

Ogni rete di computer, dalle più piccole che collegano pochi computer alle più estese come Internet, deve essere protetta da accessi non autorizzati. Per questo motivo **gli utenti si devono identificare digitando un nome utente e una password**.

La **password** tutela la privacy e la sicurezza dei dati. Assieme ad essa viene in genere chiesto di digitare anche un **nome utente**, che spesso corrisponde al vero nome dell'utilizzatore, alla sua casella di posta elettronica o a una sigla da lui scelta. Il nome utente (in inglese *user name*) è anche detto *ID utente* o *user ID* oppure semplicemente *ID* (in tutti i casi, ID deriva dalle prime due lettere della parola "Identificativo").

A differenza della password, l'ID utente non svolge un compito di protezione (tant'è vero che, quando lo si digita, le lettere appaiono sullo schermo, mentre nel caso della password vengono in genere visualizzati solo degli asterischi) ma serve – come d'altra parte dice il nome stesso – a riconoscere la persona che chiede di accedere a un sistema o a dei dati per poi richiedere l'inserimento della password associata a quell'ID.

Questa procedura di autenticazione per accedere a una rete o a un sistema informatico è detta **login** e ad essa corrisponde una successiva procedura di disconnessione detta **logout**, altrettanto importante. Al termine del collegamento è infatti indispensabile disconnettere l'account, per evitare che altre persone che utilizzano dopo di noi il dispositivo abbiano accesso a nostro nome ai servizi di rete.

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

Poiché qualsiasi password può essere individuata a causa di una disavvertenza dell'utilizzatore o dell'utilizzo di tecniche di pirateria informatica, per il controllo degli accessi si utilizzano anche **tecniche di sicurezza biometriche**, vale a dire metodi di riconoscimento che utilizzano caratteristiche fisiche uniche di un individuo per consentirne l'accesso a un sistema informatico.

Già molti dispositivi mobili permettono di utilizzare la **scansione delle impronte digitali** come sistema di accesso, mentre altri sistemi (come la **scansione dell'iride dell'occhio**) richiedono apparecchiature costose e sono quindi utilizzati solo per proteggere l'accesso a reti e servizi di importanza fondamentale, spesso di tipo militare.

Tecniche meno sicure sono il **riconoscimento facciale** e l'analisi della **geometria della mano**, in quanto espongono a maggiori rischi di fallimento dell'identificazione (l'utente autorizzato non viene riconosciuto, ad esempio se indossa una mascherina a scopi sanitari) o identificazione sbagliata (viene concesso l'accesso a utenti non autorizzati).

Il riconoscimento facciale è più che altro utilizzato per individuare e riconoscere dei visi umani all'interno di immagini fisse o in movimento. *Facebook*, ad esempio, utilizza un software che analizza tutte le foto inserite da circa un miliardo di profili per suggerire agli utenti i nomi da "taggare" confrontandoli con quelli dei conoscenti.

La geometria della mano, invece, è basata su caratteristiche come la lunghezza delle dita, l'ampiezza, lo spessore e particolari curvature della mano. È una tecnologia relativamente esatta, ma non si basa su un numero di dati numerosi come nel caso dell'impronta digitale o dell'iride dell'occhio. Inoltre, richiede appositi lettori sui quali gli utenti devono posizionare la mano, allineata rispetto a degli indicatori che favoriscono il corretto posizionamento di pollice, indice e polso.

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

Per garantire un buon grado di sicurezza, **la password** deve rispettare alcune linee di condotta:

- **non deve essere comunicata ad altri**, per nessun motivo; ciò non significa solamente non comunicarla a voce, ma anche non appuntarla in luoghi accessibili ad altri o prevedibili, come il retro del tappetino del mouse o un foglietto attaccato al monitor o lasciato nel cassetto della scrivania;
- **va modificata a intervalli regolari**, ad esempio ogni 2-3 mesi (in modo che, anche se individuata, non possa essere usata molto a lungo). In particolare, se avete bisogno di comunicare la password a chiunque per un qualunque motivo, provvedete poi a cambiarla in tempi brevissimi. Se una password vi è stata data dal gestore del sistema, cambiatela la prima volta che vi collegate.
- **va scelta sufficientemente lunga** (almeno 8 caratteri), utilizzando al suo interno minuscole e maiuscole, numeri e caratteri speciali (ad es.: "M@rio673", oppure "3nr1c0*!", ecc.) evitando però le lettere accentate, che sono differenti in base a tastiera e sistema operativo. A volte è comunque necessario raggiungere un compromesso tra l'importanza dei dati protetti, le vostre capacità mnemoniche e la sicurezza in senso assoluto della parola usata: la password non deve essere troppo difficile da digitare, altrimenti, oltre a sbagliarla spesso, dovrete digitarla lentamente, il che potrebbe favorire chi vi osserva per rubarla;
- è preferibile **utilizzare password diverse per servizi diversi**. Una buona norma è utilizzare una password per l'accesso a servizi meno importanti e un'altra più complessa per accedere a dati particolarmente riservati (gestione del proprio conto corrente, della casella di posta elettronica, ecc.).

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

Il crescente utilizzo dei servizi online conduce a un parallelo aumento del numero delle password che un utente deve ricordare per accedere a molti di questi servizi.

Sono stati perciò creati **software di gestione delle password** che, al di là di alcune differenze, svolgono la **funzione** di memorizzare tutte le password e di renderle automaticamente disponibili dopo che l'utente inserisce la cosiddetta "master password", vale a dire la password legata al software di gestione.

L'esempio più semplice è quello dei software di gestione delle password integrati nei principali browser: *Chrome, Edge,* ecc. Molti avranno notato che quando effettuiamo il login a un sito, inserendo i nostri nome utente e la password, il browser ci chiede se vogliamo che quei dati siano memorizzati per essere poi inseriti automaticamente dal browser quando ci ricollegheremo a quel sito (fig. successiva).

Si tratta di un servizio indubbiamente utile, ma non privo di **limitazioni e rischi**.

Ad esempio, se il dispositivo fosse lasciato incustodito e acceso, oppure ci fosse rubato, estranei potrebbero accedere a siti protetti da noi visitati, utilizzandone le funzioni.

Inoltre, i browser offrono l'utile funzione di sincronizzazione dei dati, che permette di ritrovare tutte le proprie impostazioni (preferiti, cronologia di navigazione, archivio delle password inserite, ecc.) anche se accediamo al browser con altri dispositivi.

In questo caso, però, estranei che riescano ad accedere all'account del nostro browser avrebbero a disposizione tutte le nostre password. È un'eventualità tutt'altro che remota, legata non solo allo smarrimento o al furto del dispositivo. Infatti, è frequente collegarsi a Internet utilizzando un dispositivo non nostro, ma dell'azienda o della scuola di cui facciamo parte, oppure di un conoscente, aprire il browser, identificarci con la nostra password… e alla fine dimenticarci di scollegarci una volta terminata la navigazione o – ancora peggio – di rifiutare il salvataggio della nostra password quando ci viene richiesta!

In generale, software di gestione delle password possono essere distinti fondamentalmente in:

- password manager online, che memorizzano le informazioni dell'utente in database criptati, conservati nei server dell'azienda produttrice del software. Per accedere al proprio database si ha quindi bisogno di una connessione a Internet, che permette di collegarsi al sito dell'azienda per inserire una "master password" che consentirà al programma di inserire automaticamente i dati richiesti quando si visiteranno siti che richiedono l'autenticazione.
- password manager desktop-based, che salvano i dati nel computer che utilizzano invece che nei server dell'azienda, col vantaggio di conservare i dati in locale e lo svantaggio di non poterci accedere da altri dispositivi e di non poter sincronizzare le informazioni.

In tutti i casi, qualsiasi sia il software scelto per gestire le password, è fondamentale scegliere una "master password" sicura, che non coincida con nessuna delle password che solitamente adoperiamo.

5 Uso sicuro del Web

5.1 IMPOSTAZIONI DEL BROWSER

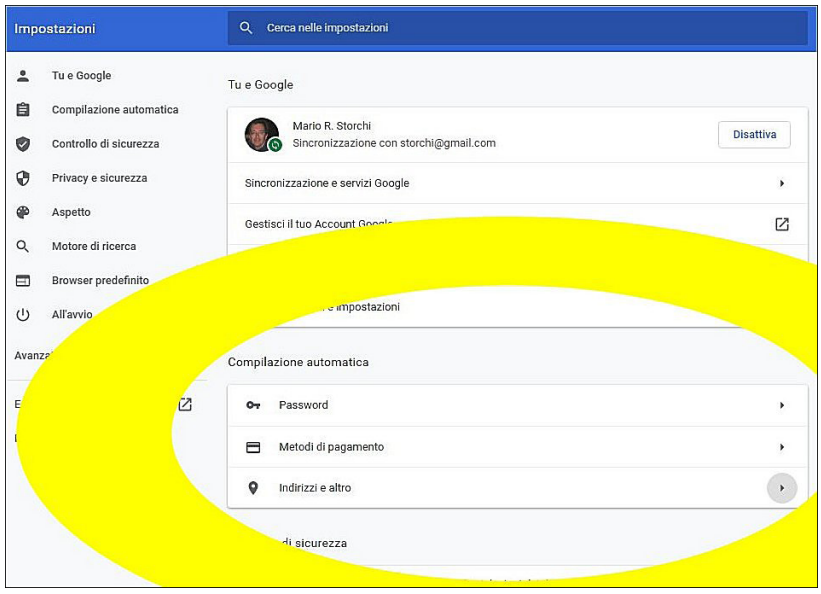
5.1.1 Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo

Quando tramite Internet vogliamo iscriverci a un servizio oppure effettuare un acquisto, dobbiamo compilare un modulo composto da una serie di caselle nelle quali ci sono chieste delle informazioni: nome, indirizzo, metodo di pagamento, ecc. Per agevolarci, il browser memorizza i dati che inseriamo, in modo da poterceli riproporre quando compileremo un altro modulo.

Questa funzione è indubbiamente comoda, ma può risultare pericolosa se non siamo gli unici a usare quel dispositivo. In particolar modo se utilizziamo il computer di un ufficio, di una scuola o di un qualsiasi locale dove sono disponibili computer con accesso a Internet gratuito o a pagamento, oppure se prestiamo il nostro dispositivo a un conoscente, nel momento in cui la persona estranea si accingerà a compilare un modulo, potrà prendere visione dei dati già inseriti in precedenza, che gli appariranno in un menu a discesa (fig. a lato).

Occorre, perciò, conoscere come **attivare o disattivare il completamento automatico dei moduli**.

Se utilizziamo ***Google Chrome*** dovremo cliccare prima su *Personalizza e controlla Google Chrome* (l'icona in alto a destra con tre puntini), poi su *Impostazioni* per aprire l'omonima pagina nella quale troveremo la sezione *Compilazione automatica* con le sezioni *Password, Metodi di pagamento, Indirizzi e altro* (fig. successiva). In ognuna di queste sezioni potremo disattivare il salvataggio e la compilazione dei dati.



Anche con ***Microsoft Edge*** occorre selezionare *Impostazioni e altro* (l'icona in alto a destra con tre puntini), poi *Impostazioni* per trovare le sezioni *Password, Info di pagamento, Indirizzi e altro,* aprendo le quali potremo attivare o disattivare il salvataggio dei dati.

Con ***Firefox*** dovremo cliccare prima su *Apri menu* (icona in alto a destra con tre linee orizzontali) e poi su *Opzioni*. Nella finestra che si apre, cliccheremo su *Privacy e sicurezza* e attiveremo, alla voce *Impostazioni cronologia*, *Utilizza impostazioni personalizzate*. A quel punto potremo scegliere se utilizzare sempre la navigazione anonima (che non conserva traccia dei siti visitati) oppure quali parti della navigazione (cronologia dei siti visitati, dati dei moduli, cronologia delle ricerche) vogliamo memorizzare e quali no. Per disattivare il salvataggio delle password dovremo utilizzare, nella stessa pagina, la sezione *Credenziali e password*.

In ***Internet Explorer*** occorre cliccare prima sull'icona *Strumenti* (in alto a destra, ha la forma di un ingranaggio), poi su *Opzioni Internet*, quindi sulla scheda *Contenuto*, al cui interno troveremo la sezione *Completamento automatico* col rispettivo pulsante *Impostazioni* che ci consente di aprire la finestra *Impostazioni Completamento automatico*, al cui interno potremo scegliere se abilitare o disabilitare il completamento dei moduli ed anche, specificatamente, il nome utente e le password.

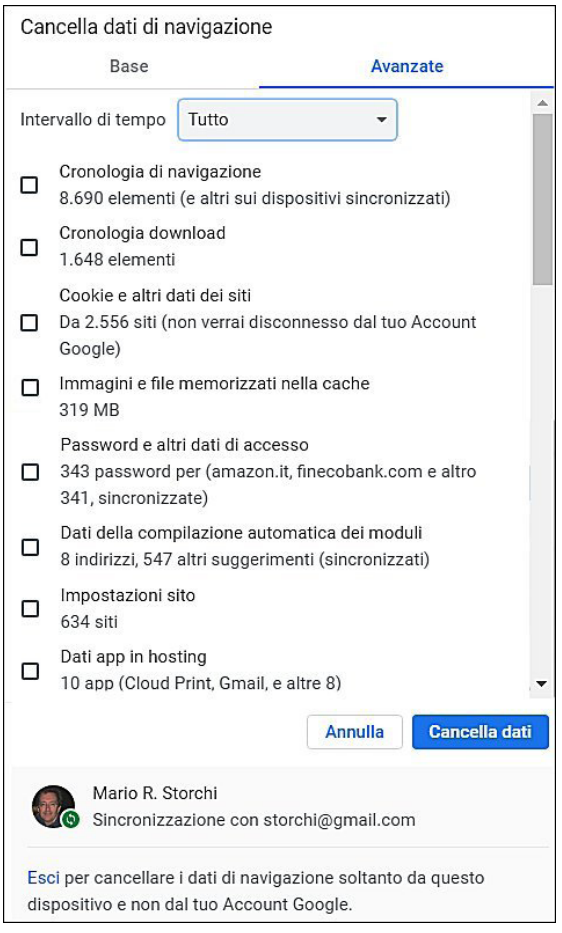
5.1.2 Eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di internet, password, cookie, dati per il completamento automatico

I browser memorizzano l'indirizzo delle pagine web che abbiamo visitato, con la possibilità di ricollegarsi a esse cliccando sui relativi link. Per visualizzare questo elenco:

- **con *Chrome*** si sceglie *Personalizza e controlla Google Chrome* (icona in alto a destra con tre puntini) e poi *Cronologia*; è anche utilizzabile la scorciatoia attraverso i tasti *Ctrl* e *H* premuti contemporaneamente;
- **con *Microsoft Edge*** e ***Internet Explorer*** occorre selezionare prima l'icona a forma di stella in alto a destra e poi la scheda *Cronologia*; è possibile anche aprire direttamente la cronologia premendo contemporaneamente i tasti *Ctrl* e *C* (con *Edge*) oppure i tasti *Ctrl* e *H* (con *Explorer*);
- **con *Firefox*** la procedura è *Apri menu* > *Libreria* > *Cronologia* e anche in questo caso è possibile aprire la finestra premendo contemporaneamente *Ctrl* e *H*.

Oltre agli indirizzi delle pagine web visitate, il browser memorizza altre informazioni per evitarci di doverle digitare nuovamente (ad es. le password salvate o le informazioni inserite nei moduli web), oltre alla cronologia dei file che abbiamo eventualmente scaricato, ai cookie, ai file temporanei che servono ad esempio in caso di blocco del computer o dell'applicazione, ecc.

Se si desiderano **cancellare queste informazioni con *Chrome*** (ad es. per evitare che altre persone possano visualizzarle, in particolar modo se abbiamo navigato utilizzando un dispositivo non nostro, ma di un amico, di un collega, di un laboratorio di informatica o di un ufficio) occorre cliccare prima su *Personalizza e controlla Google Chrome* > *Cronologia* > *Cronologia* > *Cancella dati di navigazione* e scegliere quali elementi cancellare (fig. a lato).



Con *Microsoft Edge*, selezioneremo prima il pulsante *Impostazioni e altro ancora*, poi *Impostazioni* e quindi (nella colonna di sinistra) *Privacy e servizi* per poi scorrere la pagina per arrivare alla sezione *Cancella dati di navigazione* e cliccare su *Scegli cosa cancellare*.

Con *Internet Explorer* occorre cliccare prima su *Strumenti* e poi su *Opzioni Internet*. Nella parte centrale della finestra che compare cliccate sul tasto *Elimina* che si trova nella sezione *Cronologia esplorazioni*.

Con *Firefox* la procedura è *Visualizza cronologia, password salvate e altro ancora*l > *Cronologia* > *Cancella la cronologia recente*. Anche in questo caso potremo scegliere tra diverse opzioni per cancellare tutti i dati o solo alcuni a nostra scelta. È anche possibile accedere direttamente a *Cancella cronologia recente* premendo contemporaneamente i tasti *Ctrl Maiusc* e *Canc*.

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'utilizzo di una connessione di rete sicura

Quando utilizziamo un dispositivo elettronico (computer, smartphone, tablet o altro) **collegato a una rete** (sia essa piccola – come quelle di uffici, aziende o scuole – oppure la rete più estesa di tutte: Internet) dobbiamo tenere ben presente che **i nostri dati**, inviati o ricevuti, **possono essere intercettati** da altre persone collegate a quella rete.

Per questo motivo, **alcune attività** – ad esempio quelle che implicano movimenti di denaro per acquisti online, transazioni finanziarie o altro – **devono essere eseguite solo su pagine web "sicure"**, che adottano, cioè, tecniche di cifratura dei dati, in modo che chi eventualmente dovesse intercettarli, vedrebbe solo una serie di caratteri senza senso, in quanto non possiede la chiave per decriptare i dati (della cifratura abbiamo parlato al punto 1.4.2).

Per questo motivo, una volta terminata l'attività (acquisto, transazione finanziaria o altro) occorre **scollegarsi dal sito** attraverso la procedura di *logout* o, almeno, chiudendo la pagina web. In caso contrario, chiunque avesse la possibilità di usare il computer o il dispositivo dal quale abbiamo operato, potrebbe usare i nostri dati, compresi quelli di eventuali carte utilizzate per pagamenti.

Altrettanto importante è **utilizzare una connessione sicura**, che richiede una chiave di sicurezza di rete o una password per collegarsi. Esistono anche reti aperte che permettono la connessione libera, ma occorre tener presente che in questo caso altri utenti potrebbero essere in grado di rilevare tutte le operazioni che eseguiamo: siti visitati, documenti aperti, nomi utente e password utilizzati.

Per sapere se una rete è sicura o meno, basta controllare la presenza accanto al nome della rete della parola "protetta" oppure "aperta" (in giallo nella fig. successiva), o – in altri casi – della presenza o meno dell'icona di un lucchetto. In ogni caso, cliccando sulla rete alla quale vogliamo collegarci, ci verranno fornite ulteriori informazioni.

5.2.2 Identificare le modalità con cui confermare l'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

Con Internet è possibile accedere a una quantità enorme di informazioni, ma non tutte sono sicure e affidabili, perché **ognuno ha la possibilità di inserire online informazioni fuorvianti o false**.

Se trent'anni fa uno studente di scuola media doveva eseguire una ricerca scolastica sui campi di concentramento nazisti, utilizzava principalmente enciclopedie o libri che erano a sua disposizione: nella maggior parte dei casi la scelta era spesso tra un paio di possibili fonti. Oggi, uno studente che cerca su *Google* "campi di concentramento" riceve come risultato oltre mezzo milione di indirizzi di siti web, ma tra essi ce ne sono alcuni inattendibili, per cui rischia di portare a scuola (ed è già avvenuto) una ricerca nella quale sostiene che i campi di concentramento sono una leggenda, non sono mai esistiti, perché ha utilizzato uno dei siti cosiddetti "negazionisti".

Per questo motivo è fondamentale valutare l'attendibilità delle notizie presenti in rete, tenendo ad esempio conto della **tipologia del sito** (informazione, intrattenimento, opinione, vendita) dalla quale dipende in gran parte lo scopo del sito stesso (informare, divertire, persuadere, vendere).

Se cerchiamo notizie prima di effettuare un viaggio all'estero è ben diversa l'attendibilità delle informazioni sull'argomento che possiamo trovare sui siti del Ministero degli Affari Esteri o dell'ACI rispetto a quelle fornite da un'agenzia di viaggio, specie se sconosciuta, perché in quest'ultimo caso è prevedibile che l'interesse principale sia quello di farci divenire suoi clienti.

Un elemento fondamentale di cui tener conto è l'**autore dell'informazione**, perché la credibilità di un sito è diversa a seconda che esso sia realizzato da un individuo privato, da una azienda, da un ente, da una istituzione.

Lo stesso indirizzo del sito ci aiuta spesso a capire chi ne è l'autore:

- se in esso troviamo nomi di persona (ad es. www.luigilamberti.it) o nomi di blog o spazi personali (ad es. storchi.blogspot.it) è molto probabile che si tratti di siti personali, cioè realizzati e curati da una singola persona, per cui l'attendibilità delle informazioni presenti deve essere valutata con molta attenzione;
- se l'indirizzo del sito è costituito dal nome di una istituzione conosciuta (www.protezionecivile.org.it), di una università (www.luiss.it), di una testata giornalistica (www.repubblica.it), di una società o di un soggetto commerciale noto (www.fiat.it), la loro credibilità è paragonabile a quella del soggetto stesso.

Per valutare l'autorevolezza e l'attendibilità dell'autore o del soggetto che pubblica il sito o che comunque ha messo online un'informazione, possiamo anche cercare in *Google* l'autore o il nome dell'organizzazione che pubblica il sito, oltre a tener conto della popolarità del sito e delle opinioni sullo stesso che possiamo trovare in forum dedicati al settore che riguarda quel sito.

Altro elemento fondamentale è la presenza o meno dell'**indicazione delle fonti dalle quali sono tratte le informazioni** riportate, perché questo consente di individuare l'origine dell'informazione e di verificarne validità e attendibilità. Ovviamente, le fonti indicate devono essere conosciute o almeno verificabili. Se, ad esempio, in un sito web trovo un'informazione del tipo "nel 2022, le vendite delle auto in Italia sono diminuite del 19,87% rispetto all'anno precedente" l'attendibilità è ben diversa se è indicata come fonte una pagina web che mi porta al "Rapporto ACII - Censis 2023" o piuttosto se non è indicata nessuna fonte o un riferimento del tutto generico del tipo "come ha affermato il telegiornale".

È utile **confrontare tra loro più fonti online**, tenendo però conto che le informazioni presenti in molti siti sono semplicemente una copia (a volte leggermente modificata, altre volte perfettamente identica) di informazioni tratte da altri siti e talmente replicate da rendere perlopiù impossibile capire quale sito ha pubblicato per primo l'informazione originale.

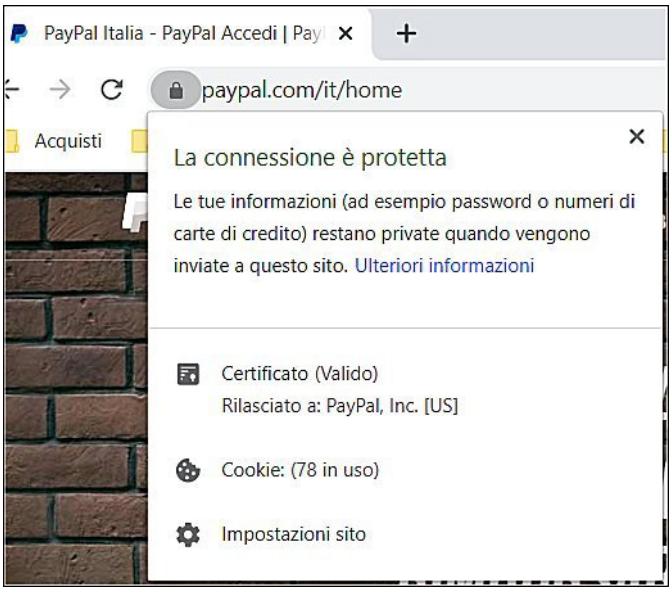
Allo stesso modo, è consigliabile **confrontare l'informazione online con una fonte tradizionale** come un'enciclopedia, un libro o una pubblicazione comunque cartacea. L'editoria tradizionale, infatti, offre maggiori garanzie di affidabilità e qualità dei contenuti.

Infine, si deve tener conto dell'**aspetto di insieme del sito web** nel quale abbiamo trovato l'informazione. Anche se non si tratta di una regola assoluta, un sito graficamente ben realizzato, che presenta link tutti funzionanti, il cui ultimo aggiornamento è recente, ha un maggior grado di credibilità.

La maggior parte delle pagine web adotta il cosiddetto "protocollo http", nel quale i dati sono trasmessi senza alcuna cifratura.

Sempre più siti, però, utilizzano la crittografia per garantire la massima riservatezza delle transazioni.

Lo stesso browser ci indica se ci troviamo in questi che sono definiti **siti web sicuri**, facendo comparire nella barra degli indirizzi **l'immagine di un lucchetto** chiuso (fig. successiva). Inoltre, nella barra degli indirizzi il nome del sito sicuro non comincia con http ma con **https**: la "s" finale è l'iniziale di *secure*, vale a dire "sicuro". Questo indica che i dati scambiati in quella pagina sono criptati.



Per assicurare l'autenticità di un sito può anche essere utilizzato un **certificato di sicurezza** emesso da un'autorità di certificazione che controlla e garantisce l'identità dell'intestatario del sito web. In questo modo, è più facile garantirsi dal pharming (punto 5.2.3).

Per visualizzare il certificato di sicurezza e altre informazioni basta cliccare sull'icona del lucchetto chiuso che compare nella barra di stato del browser. Questa procedura è detta **validazione** perché, quando clicchiamo sull'icona del lucchetto, viene inviato al sito un testo crittografato con la chiave pubblica riportata nel certificato. A quel punto, solo se il sito è quello originale, potrà rispondere con la sua chiave privata per far comparire il messaggio di verifica dell'identità.

5.2.3 Comprendere il termine "pharming"

Una truffa telematica molto diffusa per rubare dati riservati (come numero della carta di credito, password e altro) è il **pharming**, che consiste nel creare pagine web che graficamente riproducono siti famosi, per convincere le persone a digitarvi dati personali e finanziari.

Ad esempio, è possibile ricevere mail apparentemente inviate da banche, siti di vendita on-line o altre aziende famose che ci invitano a collegarci al loro sito per risolvere problemi di sicurezza (ad es. c'è bisogno di confermare o cambiare la propria password) o per approfittare di eccezionali offerte (ad es. solo per quel giorno, chi ricaricherà la propria carta di pagamento di una piccola somma di denaro, riceverà in omaggio una somma pari o addirittura maggiore), oppure per effettuare operazioni importanti e non rimandabili (fig. successiva).


Oggetto: **Postepay- telegramma urgente . - 69562-2863-77284**
Da: alerta12715@13252-secure.BPOLit
A: <f.pacelli@libero.it>

Gentile Cliente Poste Italiane ,
Notifica invio telegramma (n. di accettazione: **82150-86376-41495)**

Accedi telegramma urgente online

Queste mail contengono al loro interno uno o più link che apparentemente dovrebbero condurci al sito di quella banca o di quella azienda. In realtà, il link ci condurrà a un falso sito che cerca di imitare il più possibile quello originale, per spingerci a inserire con fiducia i nostri dati personali, che saranno intercettati da questi pirati informatici, che potranno adoperarli a loro piacimento. Altre volte, il link scarica nel nostro dispositivo elettronico un malware che consente al pirata informatico di accedere al nostro dispositivo.

I provider filtrano la maggior parte di questo tipo di mail, i programmi antivirus bloccano buona parte dei malware, gli stessi browser ci segnalano se il sito al quale stiamo per collegarci non risulta affidabile, ma resta comunque alta la possibilità di capitare in questi falsi siti.

Per questi motivi, un'ottima abitudine è dare un'occhiata alla barra degli indirizzi del browser: se in essa compaiono "https" e il simbolo del lucchetto, abbiamo la pressoché totale certezza di trovarci in un sito sicuro.

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

Con la crescente diffusione di Internet è aumentata l'esigenza di **controllare i contenuti e i tempi della navigazione**. Ad esempio, in scuole o uffici si cerca spesso di impedire che studenti o impiegati perdano tempo o utilizzino la connessione per motivi non utili allo studio, al lavoro o addirittura illegali (ad es. per scaricare contenuti protetti da diritti d'autore). Anche nelle abitazioni private, può essere utile ai genitori controllare la navigazione di figli minorenni.

Da tempo, perciò, esistono **software in grado di analizzare il contenuto dei siti visitati per impedirne il collegamento**. Alcuni di questi software impediscono lo scaricamento di determinati tipi di file (ad es. programmi, file video oppure audio, ecc.), altri l'accesso ad alcuni siti (ad es. social network, oppure siti contenenti materiale vietato) digitati dall'amministratore di rete in una apposita lista detta "black list".

Quando sono progettati principalmente per l'utilizzo da parte dei genitori, si parla di **software parentali**, che in genere aggiungono alle precedenti opzioni anche la possibilità di stabilire fasce orarie nelle quali è consentita o non consentita la navigazione in Internet.

6 Comunicazioni

6.1 POSTA ELETTRONICA

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

La posta elettronica è un mezzo di comunicazione indispensabile per privati e imprese, ma non privo di rischi di sicurezza.

Anche se per accedere alla propria casella mail occorre inserire un nome utente e una password, **la segretezza dei dati trasmessi e ricevuti non è mai garantita al cento per cento**. Normalmente, le mail sono inviate in chiaro e quindi possono essere lette da malintenzionati che le intercettino tra il loro invio e la ricezione. Gli stessi provider da cui parte e da cui è ricevuta la mail sarebbero in grado di leggerla, anche se questa operazione è vietata dalla legge. Per fare un paragone con la posta tradizionale, i normali messaggi di posta elettronica non sono come lettere chiuse, ma come cartoline, che è possibile leggere senza doverle aprire.

Per rendere sicuro un messaggio di posta elettronica è possibile cifrarlo, in modo che solo il destinatario – in possesso della chiave di decodifica necessaria – possa decifrarlo.

6.1.2 Comprendere il termine "firma digitale"

Alcuni programmi e siti permettono di inviare mail falsificando il mittente. Ciò può essere utilizzato per scherzi innocenti (spedendo, ad esempio, a un amico una mail che ha come mittente il presidente degli USA) ma anche per tentativi di truffa.

Perciò, per garantire una identificazione sicura del mittente di una e-mail, è possibile ricorrere alla **firma digitale**, un'informazione che viene aggiunta a un documento elettronico e che è rilasciata, a pagamento, da un'apposita autorità di certificazione che attesta con sicurezza l'identità del richiedente. Volendo fare un paragone con la posta tradizionale, è come spedire una raccomandata invece di una normale lettera.

In pratica, quando riceviamo una mail dotata di firma digitale possiamo consultare il certificato relativo a questa firma ed essere sicuri che il messaggio è stato inviato dal mittente indicato e che non è stato modificato.

6.1.3 Identificare i possibili messaggi fraudolenti o indesiderati

È molto probabile **ricevere nella propria casella di posta elettronica delle e-mail non richieste**, spediteci da persone venute a conoscenza del nostro indirizzo. Spesso si tratta di proposte commerciali: vendita di medicinali dall'estero, di imitazioni di prodotti di lusso, pubblicità di siti pornografici, offerte di lavoro a domicilio, pubblicità di casinò stranieri, ecc. In altri casi possono riguardare avvisi di presunti virus, offerte di denaro contante, richieste di un numero di conto corrente per ricevere soldi dall'estero , avvisi di vincite di premi o denaro, possibili donazioni o eredità, oppure mail da presunte ragazze che ci chiedono di cliccare su un link per vedere le loro foto intime.

Si tratta del fenomeno chiamato **spam**. Per chi effettua gli acquisti proposti da questo tipo di mail non c'è solo il rischio di pagare per qualcosa che non riceverà mai, ma anche di essere coinvolto in un procedimento penale, in quanto la dogana controlla le spedizioni che arrivano dai paesi extracomunitari.

Oltre allo spam è frequente ritrovare nella propria casella di posta elettronica **altri messaggi non richiesti**: alcuni provocano solo perdita di tempo (ad es. le cosiddette "catene di Sant'Antonio", che invitano il destinatario a inoltrare lo stesso messaggio a decine di altri indirizzi), ma altri possono contenere allegati o link che nascondono virus o altri tipi di malware, oppure essere dei tentativi di *phishing* (punto 6.1.4) che vogliono spingere a fornire inconsapevolmente dati riservati a scopo di truffa.

Le stesse società che ci mettono a disposizione la casella di posta elettronica, cercano di filtrare i messaggi che ci giungono, bloccando o segnalando come possibile spam messaggi di questo tipo; esistono poi diversi software che si occupano di questo servizio, a cominciare dagli stessi software di posta elettronica, che prevedono al loro interno dei sistemi anti-spam che cercano di individuare i messaggi fraudolenti per spostarli in cartelle denominate *spam, posta indesiderata* o simili.

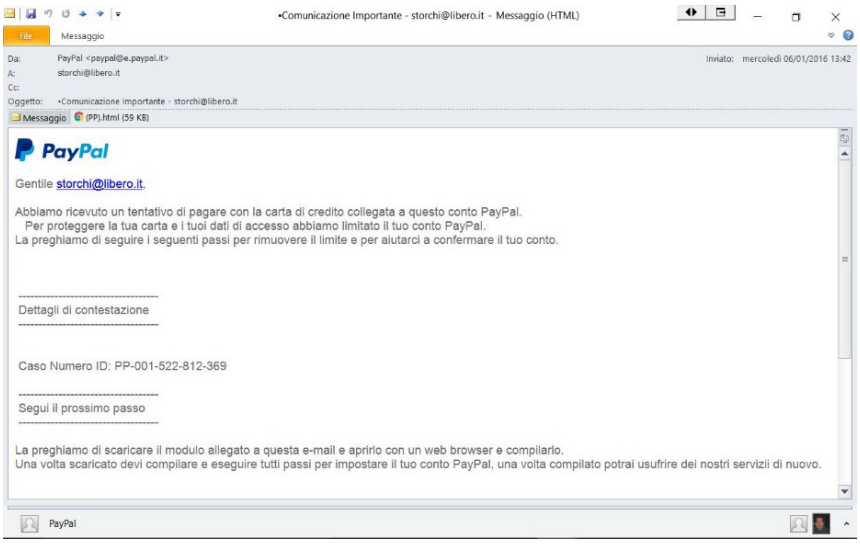
Questo, purtroppo, non garantisce in assoluto dal ricevere messaggi indesiderati e potenzialmente pericolosi. Nella migliore delle ipotesi si spreca del tempo per cancellare questi messaggi, nel peggiore dei casi si può essere infettati da virus o coinvolti in tentativi di truffe.

Non bisogna mai rispondere mai a questo tipo di messaggi, neppure per scrivere che non si è interessati o per minacciare azioni legali, in quanto ciò confermerebbe ai mittenti che quell'indirizzo mail è utilizzato e quindi può essere obiettivo di altri messaggi simili. Fanno eccezione solo mail spedite da aziende attendibili, che solitamente prevedono, nelle ultime righe del messaggio, un link che permette la cancellazione dalla loro lista di indirizzi, in modo da non ricevere altri loro messaggi.

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

Con il termine **phishing** si indicano le tecniche usate da alcuni truffatori per ottenere l'**accesso illecito a informazioni personali e riservate, mediante l'utilizzo di messaggi di posta elettronica falsi** ma modificati in modo da sembrare inviati da aziende note. Tramite questi messaggi, l'utente è ingannato e indotto a comunicare dati personali: numero di carta di credito, password, ecc.

Ad esempio, si riceve una mail apparentemente proveniente dal servizio clienti di una banca, di un sito di commercio elettronico, da *PayPal*, *Poste Italiane*, ecc. (dei quali in genere compaiono anche i loghi e i marchi originali) nella quale si avvisa di un problema di verifica dati, di un controllo a campione, del rischio di disattivazione del nostro conto, della vincita di un premio o di una somma di denaro, con la richiesta di collegarsi immediatamente al sito della società, cliccando su un link contenuto nella mail, per poi inserire alcuni dati personali come account o numero di carta di credito. Cliccando sul link, la persona visualizza sul proprio schermo un sito simile a quello originale ed è quindi più facile cadere nel tranello. Una volta comunicati i propri dati personali o finanziari, questi vengono usati dai truffatori che hanno spedito il messaggio per effettuare acquisti o trasferire somme di denaro a spese del malcapitato.



Ricordate che **nessuna azienda seria chiede informazioni riservate attraverso la posta elettronica**, per cui non bisogna mai comunicare propri dati in risposta a un messaggio non richiesto.

Anche se meno diffuso, esiste anche un phishing basato sull'**uso truffaldino non di nomi di aziende, ma di persone autentiche** da noi conosciute o di persona (un amico, un parente) o di fama (personaggi noti). Il fine rimane lo stesso: rubare informazioni riservate e personali.

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

Prima di cancellare una mail contenente un tentativo di phishing, è possibile inoltrarla alla legittima organizzazione (vale a dire la vera banca, il vero sito di commercio online ecc. dai quali apparentemente proveniva il messaggio) o alle autorità preposte, per consentire loro di intervenire contro il falso sito e di informare altri utenti.

Se il tentativo di phishing ha già provocato danni, occorre intervenire tempestivamente. Ad esempio, se ci accorgiamo di pagamenti effettuati da sconosciuti con una nostra carta di pagamento (carta di credito, Bancomat, ecc.) dobbiamo immediatamente contattare la banca per chiedere il blocco della carta. Occorre poi recarsi in un Ufficio di Polizia per effettuare una denuncia, copia della quale andrà consegnata alla filiale della banca.

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

Occorre molta attenzione quando si ricevono **messaggi di posta elettronica contenenti allegati**, perché essi **possono nascondere virus o altri malware**. Costituiscono un rischio non solo i file eseguibili, ma anche documenti creati con programmi di elaborazione testi, fogli di calcolo o altro, in quanto possono contenere dei macro-virus, vale a dire del malware nascosto nelle macro che sono eseguite dai programmi con i quali apriamo i documenti allegati alle nostre mail (punto 1.4.1).

Per questo motivo occorre **controllare gli allegati di posta con un antivirus** aggiornato. Per maggiore sicurezza, se ricevete un messaggio di posta elettronica contenente un allegato e proveniente da una persona che non conoscete, valutate la possibilità di cancellare il messaggio senza aprirlo.

Prestate attenzione anche a mail apparentemente inviate da persone o aziende conosciute: l'indicazione del mittente non è infatti una garanzia assoluta, esistono numerosi sistemi per inviare una mail falsificando il mittente. Non solo: alcuni malware colpiscono proprio i programmi di posta, inviando automaticamente messaggi contenenti copie del malware a tutti gli indirizzi contenuti nella rubrica, senza che il proprietario del computer se ne renda conto.

6.2 RETI SOCIALI

La diffusione di Internet ha portato alla nascita di **comunità virtuali**, che consistono in gruppi numerosi o numerosissimi di persone, a volte appartenenti a paesi diversi, che generalmente non si incontrano nella vita reale, ma tramite Internet. Esaminiamo alcuni esempi di queste comunità online.

Le **reti sociali** (in inglese *social network*) sono comunità virtuali di persone unite da rapporti di conoscenza (anche casuali, nel senso che si può diventare "amici" semplicemente perché si ha in comune una conoscenza), studio, lavoro o altro. Per partecipare, occorre iscriversi e creare un proprio profilo personale che contiene informazioni di base (ad es. l'indirizzo di posta elettronica) e altre informazioni che servono a descrivere meglio la persona (gli interessi, il proprio lavoro, gli hobby, ecc.). Attualmente le reti sociali con maggior numero di utenti sono *Instagram*, *Facebook* e *WhatsApp* anche se quest'ultima non è propriamente una rete sociale, ma un servizio di messaggistica istantanea.

Accanto ad alcuni vantaggi, esistono diversi rischi: le reti sociali quasi sempre vendono le informazioni su gusti e idee degli iscritti, non garantiscono la privacy in quanto è possibile spacciarsi per un'altra persona, favoriscono i furti di identità grazie alle informazioni dettagliate che è possibile ricavarne, senza considerare pericoli di altri tipo, come la spersonalizzazione dei rapporti umani.

Esistono, inoltre, anche forum, chat e altre forme di comunicazione tramite Internet, che presentano alcune potenzialità e rischi simili a quelli delle reti sociali che andremo ad esaminare in questa Sezione.

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

Per il fatto stesso di mettere in comunicazione milioni di persone, Internet amplifica dei rischi presenti anche nella vita reale, per cui è indispensabile essere prudenti.

Ad esempio, così come nella vita di ogni giorno non comunicheremmo facilmente a un estraneo dati personali (il nostro numero di telefono, l'indirizzo, ecc.), quando partecipiamo a chat o ad altre comunità virtuali, bisogna fare attenzione a **non rendere pubbliche informazioni personali** che riguardano noi o persone a noi vicine, perché questo potrebbe essere sfruttato da malintenzionati per forme di molestia, prepotenza o ricatto.

In genere, per accedere a una comunità virtuale è necessaria una iscrizione che comporta la comunicazione di alcune informazioni personali. Poiché parte di queste informazioni saranno poi visualizzabili da altri utenti, è opportuno avere una certa prudenza, evitando, ad esempio, di comunicare dati personali a prescindere da quelli obbligatori, non rendendo pubblico a tutti il proprio profilo (in questo modo le informazioni che ci riguardano potranno essere visualizzate solo da persone che fanno parte della nostra cerchia di conoscenza), limitando le informazioni personali comunicate in sede di discussione, essendo prudenti nei contatti con persone estranee.

Anche la pubblicazione di immagini personali sui siti di reti sociali richiede cautela: se esse ritraggono anche altre persone, legalmente esse dovrebbero essere informate del fatto e dare la loro approvazione. Anche in altri casi, le immagini pubblicate possono rappresentare un pericolo: si sono verificati casi in cui dei ladri hanno utilizzato le foto pubblicate nelle reti sociali per identificare e studiare le abitazioni che potevano rappresentare un buon obiettivo per i loro furti.

Allo stesso modo, occorre cautela nell'esprimere sui social network le proprie opinioni politiche, religiose o sessuali, in quanto di esse rimarrà una traccia pressoché indelebile che potrebbe essere utilizzata contro di noi. Alcune società specializzate nella selezione di candidati per grandi aziende, ad esempio, in maniera ufficiale o non ufficiale "spiano" i profili dei potenziali candidati segnalando alle aziende situazioni che ritengono inconciliabili.

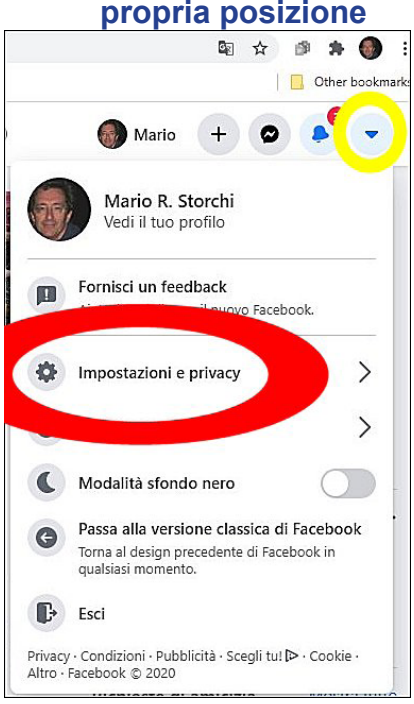
6.2.2 Essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale, quali riservatezza dell'account e propria posizione

Le reti sociali prevedono la possibilità di impostare la cosiddetta **privacy del proprio account**, in modo da scegliere chi e cosa potrà visualizzare quanto pubblichiamo. In linea di massima è consigliabile evitare che il livello di privacy del proprio account sia pubblico (in questo caso, chiunque potrebbe leggere i nostri dati personali), rendendolo accessibile solo alle persone che conosciamo nella vita reale.

Allo stesso modo, è generalmente preferibile disattivare la **geolocalizzazione**, vale a dire l'indicazione del luogo in cui ci si trova quando si invia un messaggio, una foto o un altro tipo di contenuto a una rete sociale.

Le impostazioni di privacy vanno riesaminate periodicamente, sia per adeguarle a nostre eventuali nuove esigenze, sia perché i social media modificano e arricchiscono le possibili configurazioni relative a questi aspetti.

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



Vediamo come procedere per applicare le **impostazioni degli account di reti sociali**.

In ***Facebook***, dobbiamo utilizzare la pagina *Impostazioni sulla privacy e strumenti*, che si apre in modo diverso secondo la versione che utilizziamo e se ci colleghiamo ad essa tramite un browser o direttamente con l'app. In genere occorre innanzitutto aprire il menu dell'account (indicato da un triangolo diretto verso il basso se ci colleghiamo tramite un browser, v. fig. a sinistra, oppure da tre linee parallele se utilizziamo l'app) per poi accedere o direttamente alla pagina *Impostazioni e privacy* o prima a *Impostazioni* e poi a *Privacy*.

In tutti i casi, potremo decidere chi potrà vedere i messaggi che postiamo, chi può contattarci, chi può cercarci, ecc. (fig. in basso).

È anche possibile **modificare le impostazioni di privacy nei singoli post** utilizzando due icone presenti nella finestra dei nuovi post:

la prima (evidenziata in giallo nella fig. successiva) permette di scegliere chi potrà vedere il contenuto del post (e degli eventuali allegati) che stiamo per pubblicare: tutti, solo gli amici, solo gli amici più stretti, ecc.

la seconda (evidenziata in rosso nella fig. successiva) consente di attivare/disattivare l'indicazione della posizione nel post che stiamo per pubblicare;

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

Chi utilizza le reti sociali, deve essere cosciente dei potenziali rischi:

- il **cyber bullismo**, consiste nell'utilizzo delle reti sociali per attaccare ripetutamente una persona, generalmente scelta tra quelle più deboli e riservate, con messaggi offensivi, aggressivi o minacciosi;
- l'**adescamento** (in inglese "grooming"), consiste nell'acquisire la confidenza di una persona, in genere minorenne, per spingerla a comportamenti inadeguati: appuntamenti, invio di materiale pornografico, ecc.;
- le opinioni che noi esprimiamo e più in generale tutti **i contenuti personali sono potenzialmente visibili a tutto il mondo e non più cancellabili**, perché anche se eliminiamo un nostro intervento del quale ci pentiamo, copia dello stesso rimane a disposizione dell'autorità giudiziaria nei server della società che gestisce la comunità online, senza considerare che chiunque può aver effettuato copia del nostro intervento prima della sua cancellazione. Tutto quello che inseriamo nel Web può restarci per sempre: testi, foto e quant'altro e dobbiamo essere consapevoli che, anche a distanza di molto tempo, quei testi o quelle immagini potrebbero essere letti proprio da chi non vorremmo. Inoltre, bisogna considerare il pericolo di dover rispondere anche legalmente della diffusione di informazioni false o diffamatorie, della promozione di idee o azioni illegali, oppure della diffusione di materiale protetto da copyright o dannoso (ad es. contenente malware);
- possono essere pubblicate **informazioni fuorvianti o pericolose**, a volte solo per catturare l'attenzione altrui, altre volte per secondi fini;
- possono essere create **false identità** (in inglese "fake"), utilizzate sia per adescamento sia per cyberbullismo;
- possono essere pubblicati **link o messaggi fraudolenti**, per rubare dati personali (in questo caso si tratta di una tecnica di *phishing*, v. punto 6.1.4) o per spingere a visitare determinate pagine web.

Per il fatto stesso di mettere in comunicazione milioni di persone, Internet amplifica dei rischi presenti anche nella vita reale, per cui è preferibile **non rendere pubbliche informazioni personali** che riguardano noi o persone a noi vicine, perché questo potrebbe essere sfruttato da malintenzionati per forme di molestia, prepotenza o ricatto. Teniamo sempre ben presente che le persone nella realtà possono essere molto diverse da come si descrivono in rete: spesso non abbiamo modo di sapere se la persona che si presenta a noi come un ragazzo o una ragazza sia davvero tale o, piuttosto, un adulto con cattive intenzioni.

Sempre come nella vita reale, in Internet esistono i tentativi di truffa, per cui bisogna **diffidare di proposte di acquisto o di investimento** particolarmente vantaggiose che possono pervenirci via mail. Si tratta, in diversi casi, di malintenzionati che spesso operano da paesi non raggiungibili dalla giustizia italiana.

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

Come nel caso del phishing, è possibile **segnalare comportamenti inappropriati della rete sociale al fornitore di servizi o alle autorità preposte**.

In linea generale, è preferibile ricorrere all'amministrazione della rete sociale quando troviamo contenuti offensivi o comunque inadeguati (come un linguaggio offensivo o la pubblicazione di materiale pornografico o protetto da diritti d'autore), mentre è opportuno rivolgersi alla Polizia (anche utilizzando il link www.commissariatodips.it indicato al punto 6.1.5) o ai Carabinieri, se siamo noi stessi l'oggetto di una minaccia o di un reato di altro genere.

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)

La **messaggistica istantanea** (in inglese "instant messaging", spesso abbreviata in **IM**) è un **sistema che consente di inviare e ricevere brevi messaggi in tempo reale** a uno o più interlocutori collegati in quel momento a Internet o a un'altra rete.

Utilizzando una applicazione specifica (ad es. *WhatsApp*) o un analogo servizio integrato in un'applicazione (ad es. la chat di *Facebook* o la messaggistica istantanea di *Skype*), sullo schermo del nostro dispositivo compare un riquadro ("contact list") nel quale è possibile sapere quante e quali persone che conosciamo e il cui nome abbiamo memorizzato nell'applicazione, sono in quel momento collegate come noi in rete.

A quel punto si può chattare, spedire o ricevere un file, in alcuni casi anche parlare in videoconferenza, grazie all'uso di microfono e webcam, con una o più di quelle persone. Rispetto alle mail lo scambio è quindi immediato, rispetto alle chat non è aperto a tutti, ma solo ai propri contatti.

Il termine **VoIP** deriva dalle iniziali di "Voice over Internet Protocol", che significa "voce attraverso il protocollo Internet". Si tratta di una **tecnologia che utilizza la rete Internet per effettuare telefonate**. È molto diffusa, perché assicura notevoli risparmi rispetto ai metodi tradizionali utilizzati per le telefonate, pur offrendo un'eccellente qualità audio, a patto che si utilizzi una connessione a banda larga. Le conversazioni VoIP possono usare come mezzo di trasmissione non solo internet ma qualunque rete privata basata sullo stesso principio di funzionamento, per questo motivo alcune grandi aziende utilizzano le loro reti private per creare un proprio servizio VoIP.

Come la posta elettronica, anche **la messaggistica istantanea e la telefonia VoIP comportano potenziali rischi**:

- trasmissione di malware;
- accesso a file personali o all'intero sistema attraverso l'utilizzo di *backdoor* (punto 2.1.1);
- intercettazione dei messaggi e delle conversazioni (in inglese "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

Per **assicurare la confidenzialità durante l'uso della messaggistica istantanea e della telefonia VoIP**, occorre:

- utilizzare software che assicuri la cifratura dei messaggi, in modo che possano essere letti solo dai legittimi destinatari;
- evitare di comunicare nei messaggi e nelle conversazioni telefoniche informazioni riservate o importanti;
- limitare la condivisione dei file e utilizzare un antivirus aggiornato per assicurarsi che i file ricevuti e inviati non contengano malware.

6.4 DISPOSITIVI MOBILI

I dispositivi mobili sono apparecchi elettronici facilmente trasportabili, che permettono di svolgere, anche se non ci si trova in casa o un ufficio, operazioni che fino a qualche anno fa erano possibili solo utilizzando computer fissi.

Attualmente, i dispositivi mobili maggiormente diffusi sono smartphone e tablet, entrambi dotati di collegamento a Internet e di uno schermo sensibile al tocco del dito e perciò detto "touchscreen", sul quale compare una tastiera virtuale quando è necessario digitare caratteri o parole.

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 applicazioni per dispositivi mobili vanno scaricate da siti definiti app store. Ogni sistema operativo possiede uno o più **app store ufficiali**; i più utilizzati sono *Play Store* per il s.o. *Android* e *App Store* per il s.o. *iOS* della *Apple*.

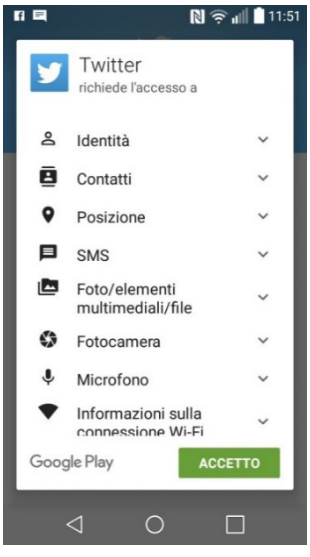
In questi siti sono disponibili sia applicazioni gratuite che applicazioni a pagamento (in genere piuttosto modesto).

Esistono anche numerosi **app store non ufficiali** che attraggono i visitatori con la promessa di scaricare gratuitamente anche le applicazioni solitamente a pagamento. A parte che questa promessa non è sempre mantenuta, occorre tenere ben presente i possibili rischi:

- trasmissione di malware espressamente progettato per i dispositivi mobili;
- consumo eccessivo e non necessario delle risorse del dispositivo, con conseguente diminuzione delle prestazioni;
- accesso a dati personali e loro eventuale trasmissione a terzi;
- scarsa qualità delle applicazioni;
- costi nascosti.

6.4.2 Comprendere il termine "autorizzazioni dell'applicazione"

Dopo aver scaricato un'applicazione per dispositivo mobile e subito prima di avviare il processo di installazione, il sistema operativo ci mostra una schermata nella quale sono elencate le diverse autorizzazioni richieste dall'applicazione (fig. successiva).



Solo dopo aver premuto il pulsante *Accetto* verrà avviata l'installazione. Praticamente tutti accettiamo le condizioni senza averle lette e questo può comportare problemi, in particolare (ma non solo) se l'app è stata scaricata da un app store non ufficiale.

Quasi ogni applicazione necessita di alcuni permessi per funzionare, legati al funzionamento dell'applicazione stessa, ma occorrerebbe valutare se sono richieste autorizzazioni non connesse al tipo di applicazione che stiamo per installare.

Alcuni esempi serviranno a fare maggiore chiarezza: se stiamo per installare una app di navigazione satellitare è normale che essa richieda di accedere alla localizzazione GPS; se l'app da installare è un social network ci chiederà l'autorizzazione ad accedere al nostro elenco contatti e probabilmente – se integra anche una funzione telefonica – anche l'autorizzazione a effettuare chiamate dirette o ad inviare SMS. Se, però, queste stesse autorizzazioni sono richieste da un gioco o da un programma di utilità (ad es. una calcolatrice, una torcia, ecc.) non è il caso di accettare senza problemi.

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

Possiamo controllare le autorizzazioni concesse anche dopo aver installato una app, andando prima in *Impostazioni*, poi in *Applicazioni* e infine selezionando l'app che ci interessa.

Scorrendo la schermata che ci appare, troveremo la sezione *Autorizzazioni* nella quale sono elencati tutti i permessi concessi a quella app; selezionando i vari permessi comparirà in genere una breve spiegazione.

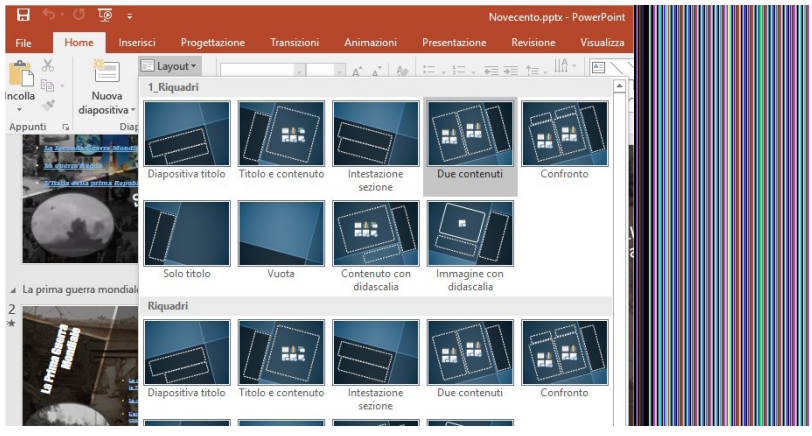
Nel caso in cui i permessi concessi non ci sembrano adeguati all'applicazione e se abbiamo notato malfunzionamenti nel dispositivo mobile, possiamo – nella parte superiore della stessa schermata – procedere alla disinstallazione della app.

Occorre prestare particolare attenzione alle seguenti autorizzazioni:

- *chiamata diretta n. telefono;*
- *acquisizione di foto e video;*
- *leggi i tuoi contatti;*
- *aggiungi o modifica gli eventi del calendario e invia e-mail a ospiti all'insaputa dei proprietari;*
- *leggi i contenuti della scheda SD. Modifica o elimina i contenuti della scheda SD;*
- *localizzazione precisa;*
- *accesso completo alla rete.*

Ripetiamo: le autorizzazioni sono necessarie alle app per svolgere le loro funzioni; quelle appena elencate, ad esempio, sono tra quelle richieste da una app nota e affidabile come *Facebook*. Se, però, una o più di queste autorizzazioni fossero presenti nella scheda di una app che ha tutt'altre funzioni, dobbiamo essere consapevoli che concediamo a quella app permessi potenzialmente pericolosi:

- poter comporre numeri a pagamento a nostra insaputa;
- accedere alle nostre foto, ai nostri video, a tutti i dettagli dei nostri contatti e a qualsiasi file è memorizzato nel dispositivo;
- conoscere la cronologia delle nostre posizioni;
- trasmettere il tutto ad altri attraverso Internet, poiché abbiamo concesso anche il permesso di accedere autonomamente alla rete.



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

Proprio per la quantità e il valore delle informazioni personali che contengono, occorre **essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile**.

Praticamente tutti i sistemi operativi per dispositivi mobili consentono di effettuare alcune operazioni sul dispositivo anche se l'abbiamo smarrito o se ci è stato rubato. Sono però necessarie alcune condizioni, in genere (ma non sempre) attivate automaticamente:

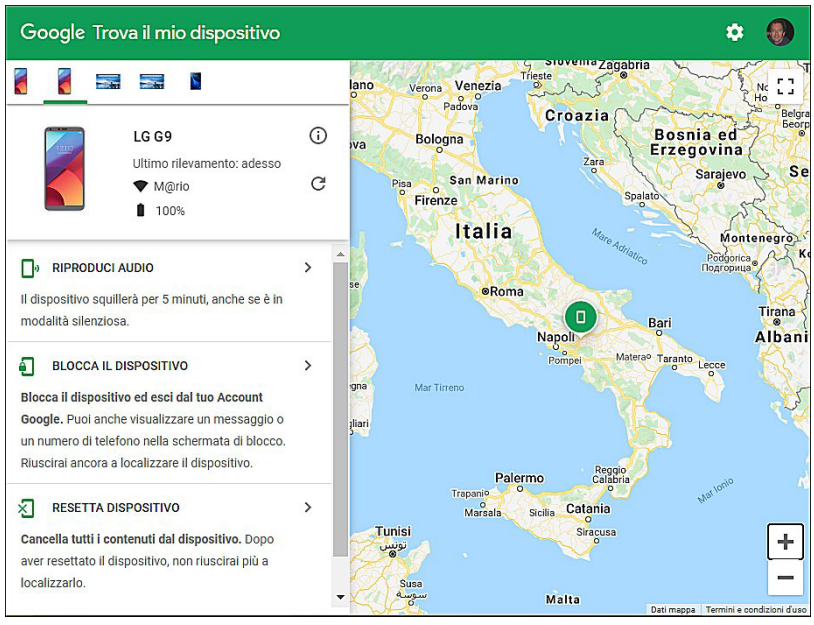
- il dispositivo deve essere associato a un nostro account;
- sul dispositivo deve essere attivata la funzione necessaria alla sua localizzazione;
- il dispositivo deve essere dotato di connessione a Internet.

Se perdiamo un dispositivo *Android*, ad esempio, dovremo accedere con un altro dispositivo al nostro account *Google* e utilizzare la funzione *Gestione dispositivi Android* oppure collegarci all'indirizzo android.com/find (fig. successiva).

A questo punto potremo:

- localizzare il dispositivo su una mappa;
- farlo squillare ininterrottamente per circa cinque minuti, selezionando *Riproduci audio*;
- bloccarlo, procedendo a una disattivazione remota, scegliendo *Blocca il dispositivo* e impostando una password che sarà poi necessaria per lo sblocco.;
- cancellare tutti i contenuti personali, scegliendo *Resetta dispositivo*. Teniamo presente che se è presente una scheda di memoria, alcuni dati potrebbero non essere cancellati e soprattutto che, dopo aver effettuato la cancellazione, non funzionerà più la localizzazione del dispositivo.

Simili sono le funzioni offerte dall'app *Dov'è*, offerta gratuitamente da *Apple* agli acquirenti dei suoi dispositivi portatili.



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

In caso di **furto di un dispositivo informatico** come tablet, portatile, smartphone o computer fisso, alla perdita dell'apparato si aggiunge la perdita dei dati in esso contenuti, con i conseguenti rischi che – se essi non sono stati adeguatamente protetti con password e cifratura dei dati – possano essere visti e utilizzati da malintenzionati.

La regola più importante per prevenire i furti è anche quella più ovvia: il dispositivo non va mai lasciato incustodito in aree pubbliche o comunque in aree dove non si può escludere la presenza di estranei.

Quando si tratta di un portatile e ci si trova ad adoperarlo frequentemente in luoghi aperti al pubblico, si possono utilizzare degli appositi **cavi dotati di lucchetto**, che da una parte si fissano al computer, dall'altro a una scrivania.

È anche opportuno **conoscere e conservare il numero di matricola** dell'apparecchio, per poterne denunciare l'eventuale furto alle autorità competenti.

Nelle aziende e nelle scuole, dove sono presenti numerosi dispositivi informatici, è necessario **registrarne, in un inventario costantemente aggiornato, i dettagli precisi e la collocazione** (ad esempio: stampante laser a colori marca… modello… numero di serie… collocata nella postazione numero… del laboratorio di informatica numero…), in maniera da poter individuare con certezza eventuali furti o manomissioni.

Allo stesso scopo, occorre **controllare gli accessi ai locali nei quali si trovano i dispositivi**, sia per evitare danneggiamenti o furti, sia per poter eventualmente risalire ai colpevoli.

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

Molte persone archiviano nei dispositivi elettronici una enorme quantità di dati, della cui importanza si rischia di rendersi conto solo quando un guasto dell'apparecchio, il suo smarrimento o furto, un nostro errore, l'azione di un malware, uno sbalzo di corrente, ci privano di informazioni e ricordi dei quali spesso non si conserva una copia aggiornata. Il malfunzionamento o la perdita di uno smartphone, ad esempio, può causare la perdita della lista dei contatti con i relativi numeri di telefono, oppure di foto scattate con quell'apparecchio e mai copiate su altri supporti di memoria. Nel caso di dispositivi più complessi, come tablet, portatili o altro, la perdita può essere più grave: documenti di studio o di lavoro, informazioni finanziarie, ecc.

Per questi motivi occorre effettuare periodicamente **copie di sicurezza o backup** su **supporti di memoria** (schede di memoria, penne USB, dischi fissi esterni, ecc.), in modo da poter recuperare i dati in caso di perdita o danneggiamento degli stessi.

È anche possibile effettuare la copia di sicurezza online, su server remoti, nel cosiddetto **cloud**, che permette anche di accedere ai backup da qualsiasi postazione collegata a Internet. Non mancano potenziali rischi, che vanno dall'attacco di pirati informatici, a malfunzionamenti del server, sino alla più semplice ma non impossibile eventualità di trovarsi in un posto dove è impossibile il collegamento a Internet, quantomeno a una velocità accettabile per accedere al backup online.

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

L'**intervallo di tempo tra un backup e l'altro** dipende dall'utente e dal tipo e dalla quantità di dati trattati: negli istituti bancari, ad esempio, si realizzano più copie di sicurezza nel corso di una stessa giornata, negli uffici o nelle piccole aziende spesso il backup viene effettuato alla fine della giornata lavorativa, per gli utenti privati può essere sufficiente aggiornare le copie di sicurezza ogni settimana o mese.

In ogni caso è fondamentale la **pianificazione**: una volta stabilito il periodo di tempo, occorre procedere sempre all'effettuazione del backup, senza eccezioni. Se i dati sono particolarmente numerosi (ad es. nel caso di medie e grandi aziende) si può ricorrere a tecniche di **compressione dei dati** per ridurre lo spazio necessario per la memorizzazione.

Inoltre, i supporti di memoria sui quali sono realizzate le copie di sicurezza dei dati devono essere rimovibili, in modo da essere conservati in luoghi sicuri e diversi da quelli dove solitamente si trova il dispositivo. In questo modo, in caso di furto o danneggiamento del dispositivo dovuto a eventi di forza maggiore (ad esempio un incendio o un allagamento che colpiscono il locale dove si trova il computer) le copie di backup non faranno la stessa fine.

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

Il modo più semplice per effettuare una copia di sicurezza dei dati è copiare periodicamente i file creati da una applicazione su di una memoria di massa diversa: ad esempio collegando una penna USB o una scheda di memoria a un dispositivo portatile, selezionando in quest'ultimo i file da copiare (documenti, foto, video) e procedendo alla copia sulla memoria di massa temporaneamente collegata al dispositivo.

È possibile effettuare la copia di sicurezza anche sulla stessa unità locale (vale a dire nella memoria dello stesso dispositivo che stiamo adoperando) oppure su un servizio cloud. Nel primo caso, però, un eventuale smarrimento, furto o guasto irreparabile del dispositivo, ci priverebbe anche della copia di sicurezza. Nel caso del cloud, invece, abbiamo bisogno di una connessione Internet.

Esistono numerosi programmi che effettuano copie di sicurezza in maniera semi-automatica, indicando solo la prima volta i file da copiare e la memoria esterna nella quale copiarli, dopo di che sarà comunque sempre possibile modificare successivamente le scelte effettuate.

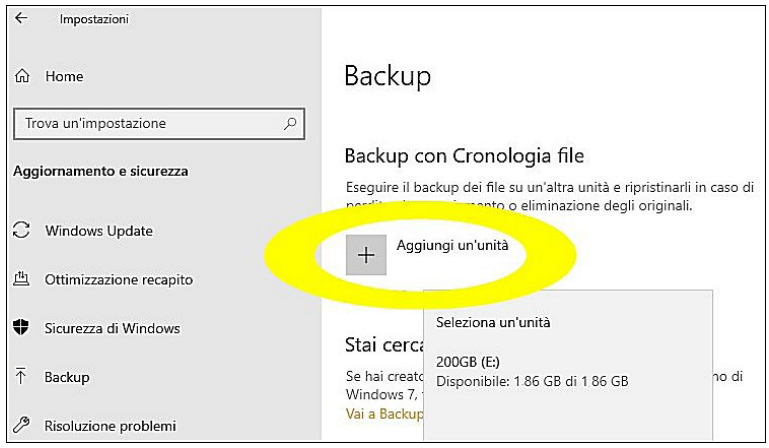
Gli stessi sistemi operativi (*Windows, Android, Apple*, *Linux*) integrano già queste app:

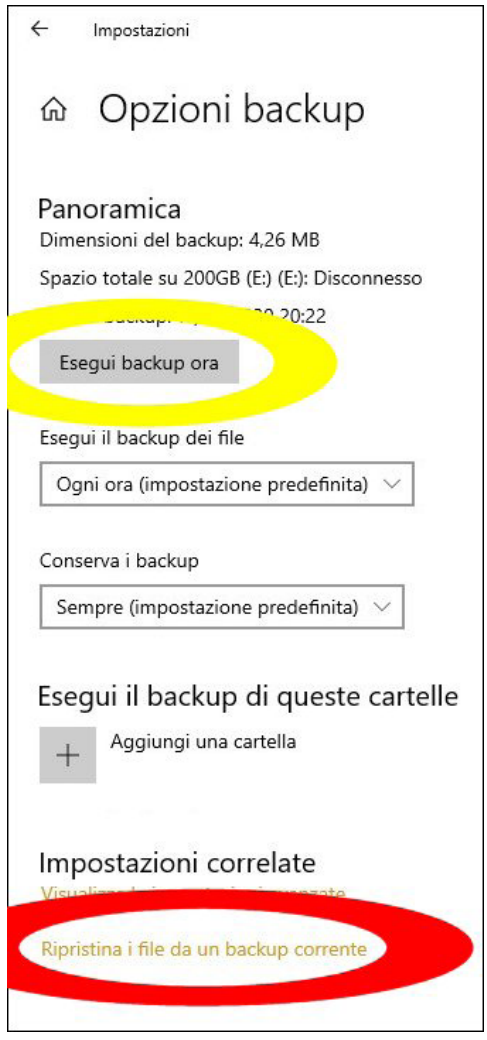
- in *Windows*, questo programma è raggiungibile da *Start* > *Impostazioni* (l'icona a forma di ingranaggio che si trova sopra a *Start*) > *Aggiornamento e sicurezza* > *Backup* oppure cominciando a digitare "backup" nella casella di ricerca sin quando non compare tra i risultati *Impostazioni di backup* su cui dovremo cliccare;
- in *Android* si trova generalmente in *Impostazioni* > *Generali* > *Backup*;
- nei sistemi *Apple*, è possibile utilizzare *iCloud*;
- in *Linux Ubuntu*, si può digitare "backup" nella *Dash*, che si apre cliccando sul pulsante di *Ubuntu* nella barra di sinistra.

Ecco, ad esempio, la procedura per effettuare il primo backup di una unità disco, utilizzando *Windows 10*:

1. cominciamo a digitare "backup" nella casella di ricerca sin quando non compare tra i risultati *Impostazioni di backup* su cui dovremo cliccare (in alternativa potremo selezionare *Start* > *Impostazioni* > *Aggiornamento e sicurezza* > *Backup*);
2. scegliamo *Aggiungi un'unità* (evidenziato nella fig. successiva) e scegliamo l'unità esterna su cui registrare il backup;

3. scegliendo *Altre opzioni* apriremo la finestra *Opzioni backup* (fig. successiva) nella quale potremo scegliere, tra l'altro, di avviare subito il backup cliccando su *Esegui backup ora.*





Teniamo presente che la procedura di backup può richiedere parecchio tempo, durante il quale il computer deve rimanere acceso e collegato alla memoria esterna nella quale sarà memorizzato il file di backup.

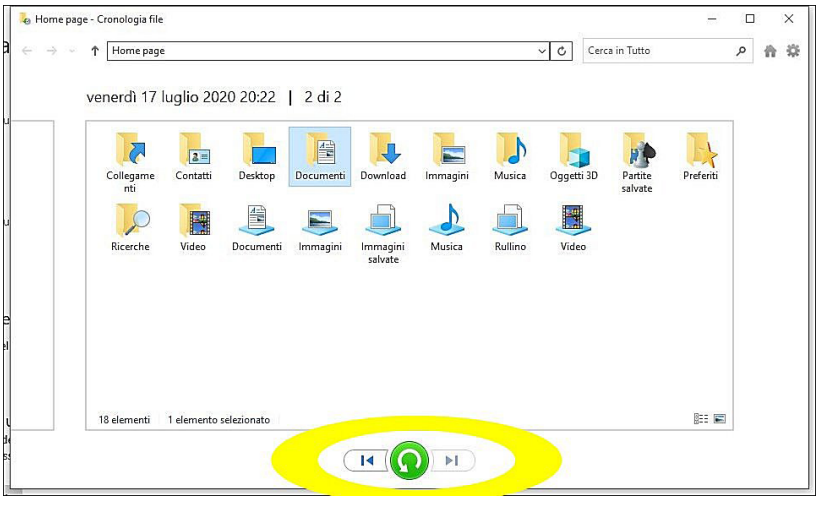
7.1.5 Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud

Se abbiamo seguito sin qui le raccomandazioni riguardanti i backup, in caso di danneggiamento o perdita di dati, potremo procedere al **ripristino** (cioè il recupero dei dati) e alla **validazione** (il controllo dell'integrità della copia) **dei dati utilizzando la copia di sicurezza memorizzata sull'unità locale** (il dispositivo che stiamo adoperando), **su una unità o supporto esterno** (come penne USB, schede di memorie o hard disk esterni), **oppure su un servizio cloud**.

Se non dobbiamo lavorare su una gran quantità di dati, il modo più semplice è quello di procedere manualmente, collegando al dispositivo il supporto di memoria sul quale abbiamo effettuato il backup più recente, individuando e selezionando i file da copiare e, infine, effettuando la vera e propria copia nella cartella preferita del dispositivo. Una volta terminata la copia, aprendo i file potremo accertarci del loro corretto funzionamento.

Gli stessi programmi illustrati al punto precedente (*Backup* in *Windows, Android* e *Linux*, *iCloud* nei dispositivi *Apple*) consentono di effettuare in maniera semi-automatica le operazioni di ripristino e validazione. In pratica, dopo aver avviato le applicazioni e individuata la copia di sicurezza più recente, i programmi ci inviteranno a confermare o scegliere la cartella nella quale verranno ripristinate le copie di sicurezza, per poi procedere alla vera e propria operazione (che non deve essere interrotta) che prevede una verifica finale.

Ad esempio, con *Windows 10*, nella finestra *Opzioni backup* troveremo come ultima scelta *Ripristina i file da un backup corrente* (in rosso nella fig. precedente) che aprirà la finestra *Cronologia file* (fig. successiva) nella quale troveremo i backup effettuati e potremo scegliere quali ripristinare utilizzando la barra di navigazione in basso (in giallo nella fig. successiva) al centro della quale il grande pulsante verde avvia il ripristino dei file o cartelle selezionati.



7.2 CANCELLAZIONE E DISTRUZIONE SICURA

7.2.1 Distinguere tra cancellare i dati ed eliminarli in modo permanente

La normale procedura di **cancellazione dei dati** è del tutto differente dall'**eliminazione permanente dei dati** stessi.

Prendendo ad esempio un computer sul quale è installato il sistema *Windows*, i dati cancellati vengono spostati in una cartella speciale, chiamata *Cestino*, dalla quale possono essere facilmente ripristinati. Anche se si provvede allo svuotamento del *Cestino*, con programmi specifici e facilmente reperibili è spesso possibile ripristinare in parte o del tutto i file cancellati. Anche se utilizziamo un tablet o uno smartphone, la semplice cancellazione dei dati non assicura in genere la loro eliminazione definitiva.

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

Quando occorre **disfarsi di un dispositivo mobile** (smartphone, tablet, notebook o altro) **o di un supporto di memoria** (disco fisso, penna USB, CD, DVD o altro) perché rotti o inutili, è importante **eliminare in modo permanente tutti i dati in essi contenuti**, sia che li si voglia buttare (in questo caso occorre contattare il proprio Comune per sapere dove e quando andrà depositato) sia che li si voglia vendere o donare ad altra persona.

Noi, infatti, spesso dimentichiamo la quantità di dati personali che sono memorizzati in un dispositivo o in una memoria di massa: foto, messaggi, cronologia dei siti che abbiamo visitato, copie di documenti di identità, numeri delle ultime conversazioni telefoniche, ecc.

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 **l'eliminazione del contenuto da servizi come reti sociali, blog e forum non è mai sicuramente definitiva**.

Ad esempio, chi ha visualizzato un messaggio che prima abbiamo pubblicato e poi cancellato, può nel frattempo averlo copiato, oppure condiviso, semmai rendendolo di dominio pubblico. Lo stesso vale per immagini e altri contenuti. Inoltre, quasi tutti i social network conservano copia di quanto pubblicato dai propri utenti, anche se successivamente cancellato, e alcuni pongono limiti nella cancellazione di quanto pubblicato.

Anche la cancellazione di contenuti caricati su un cloud può non essere permanente per diversi motivi: ad esempio se il contenuto era stato condiviso, esso viene cancellato in modo automatico solo dal nostro cloud e non da quello degli altri utenti autorizzati; inoltre molti servizi cloud effettuano copie di sicurezza dei dati, ecc.

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 utilità per la cancellazione definitiva dei dati

Per **distruggere definitivamente i dati** è necessario utilizzare metodi specifici, ad esempio:

- **triturazione dei documenti cartacei** attraverso l'utilizzo di "trita documenti" o "distruggi documenti" (esistono anche modelli molto economici) che riducono i fogli in striscioline o coriandoli;
- **distruzione delle memorie di massa o dei dispositivi** che si è sicuri di non voler più utilizzare, vendere o regalare, utilizzando un martello o un trapano che danneggino in modo irreparabile le memorie. Nel caso di CD, DVD e schede di memoria è sufficiente piegarle più volte sin quando non si spezzano. Ovviamente si tratta di operazioni da praticare con attenzione, per evitare di farsi male;
- **smagnetizzazione** (o "degaussing") attraverso apparecchi che generano campi magnetici in grado di rendere inutilizzabili le memorie di massa; questa è una pratica solitamente utilizzata da grandi aziende e non da privati;
- **cancellazione definitiva dei dati** grazie a programmi che, dopo aver cancellato i file, sovrascrivono più volte lo spazio di memoria da loro precedentemente occupato, in modo da rendere impossibile ogni recupero.