# Sicurezza informatica

Ei-book

# Premessa

Questo modulo introduce le regole e le buone prassi che consentono di minimizzare la vulnerabilità dei sistemi informatici.

Di fatto, le nuove tecnologie informatiche consentono a un numero sempre più alto di persone di svolgere sempre più attività che hanno come oggetto anche dati e informazioni sensibili.

Immagina il computer come la cassaforte delle nostre informazioni più preziose; devi gestirne con attenzione la sicurezza.

Di seguito, analizzeremo tutti i metodi di prevenzione, i comportamenti che un utente diligente deve eseguire come netiquette e le tipologie più comuni di virus informatici. Nel linguaggio di Internet, con netiquette ci riferiamo all'insieme delle norme di comportamento, non scritte ma a volte imposte dai gestori, che regolano l'accesso dei singoli utenti alle reti telematiche, spec. alle chat-lines.

www.treccani.it

Acquisiremo, quindi, le competenze e le conoscenze necessarie per identificare e affrontare le principali minacce alla sicurezza informatica.

# Disclaimer

Certipass ha predisposto questo documento per l'approfondimento delle materie relative alla Cultura Digitale e al migliore utilizzo del personal computer, in base agli standard e ai riferimenti Comunitari vigenti in materia; data la complessità e la vastità dell'argomento, peraltro, come editore, Certipass non fornisce garanzie riguardo la completezza delle informazioni contenute; non potrà, inoltre, essere considerata responsabile per eventuali errori, omissioni, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione ed eventualmente utilizzate anche da terzi.

Certipass si riserva di effettuare ogni modifica o correzione che a propria discrezione riterrà sia necessaria, in qualsiasi momento e senza dovere nessuna notifica.

L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del sito dedicate al Programma.

# 1. L'IT Security

## 1.1. Concetti di base

L'*IT Security* è l'insieme delle tecnologie con cui proteggere reti informatiche, sistemi operativi, programmi e dati, da possibili minacce molto spesso imprevedibili.

Lo scopo principale dell'*IT Security* è pertanto garantire la protezione dell'integrità fisica (*hardware*) e logico-funzionale (*software*) di un sistema informatico e dei dati in esso contenuti, minimizzandone la vulnerabilità (la vulnerabilità infatti misura il livello di esposizione del sistema rispetto alla minaccia).

Considerata la pervasività delle tecnologie informatiche nella nostra sfera privata e lavorativa, l'*IT Security* è diventato un tema centrale per tutti noi. Più tecnologie ICT (*Information and Communication Technology*) impieghiamo per svolgere le nostre attività quotidiane, più cresce il rischio di perdere o subire un furto di dati e informazioni.

### 1.1.1. Obiettivi dell'IT Security

L'*IT Security* deve poter garantire efficacemente cinque requisiti.

- *Integrità dei dati.* I dati devono effettivamente essere quelli che le parti in causa legittimamente sono convinti che siano. Soltanto le persone autorizzate devono pertanto poter modificare i dati. Il sistema informatico inoltre deve essere in grado di segnalare ogni modifica non autorizzata.
- *Confidenzialità.* Soltanto le persone autorizzate devono poter accedere ai dati, in modo che nessun altro possa vederli e diffonderli.
- *Disponibilità.* Le persone autorizzate devono poter sempre accedere ai servizi e risorse online a cui sono registrate. Il sistema informatico pertanto non deve chiedere ulteriori autorizzazioni o chiavi di accesso diverse da quelle in loro possesso.
- *Non ripudio.* Una transazione o un'azione svolta non può essere negata a posteriori dall'operatore.

- *L'autenticazione.* Verificare l'identità di un utente garantisce a ciascun corrispondente che il suo partner sia effettivamente quello che crede.

### 1.1.2. I diversi tipi di minacce

Le minacce informatiche sono riconducibili a due ordini di fenomeni: gli *eventi accidentali* e gli *eventi indesiderati*.

Gli *eventi accidentali* sono la conseguenza di situazioni non ponderabili, legate a elementi casuali. Ad esempio, i fenomeni atmosferici — soprattutto quando sono di forte intensità — possono causare l'interruzione della corrente elettrica, e pertanto possono danneggiare i dispositivi informatici, con la conseguente perdita dei dati al loro interno.

Gli *eventi indesiderati* sono le operazioni che soggetti malintenzionati eseguono per danneggiare i nostri dispositivi, e per sottrarci dati e informazioni. Possiamo così distinguere gli *attacchi malevoli*, lanciati per intaccare il funzionamento dei sistemi informatici, dagli *accessi ai dispositivi da parte di soggetti non autorizzati*, il cui scopo è sottrarre dati e informazioni dai sistemi informatici.

### 1.1.3. Crimini informatici e hacker

Attacchi malevoli e accessi non autorizzati a banche dati o memorie di archiviazione sono senza dubbio crimini informatici. Rientrano in questa categoria di crimini tutte le azioni compiute tramite l'utilizzo delle tecnologie informatiche, e che costituiscono un reato.

Avendo conoscenza di sistemi informatici, un malintenzionato può infatti compromettere, anche in maniera grave, il funzionamento di un PC (o di un altro dispositivo), e minare pertanto l'integrità, la riservatezza e la disponibilità dei dati e delle informazioni in esso immagazzinate.

A causa della natura immateriale di molte minacce informatiche, questo tipo di infrazioni sono più complesse da riconoscere, e costituiscono pertanto uno dei più importanti ambiti di studio dell'*IT Security*.

Per identificare gli autori di crimini informatici, si utilizza la parola inglese *hacker*. Come spesso accade, la traduzione in italiano delle parole inglesi non è molto precisa, almeno

rispetto al loro significato originale. È questo il caso della parola *hacker*, che inizialmente aveva un'accezione positiva. Veniva infatti utilizzata per indicare gli studiosi che cercavano di superare creativamente i problemi tecnici e operativi dei primi sistemi informatici.

Un *hacker* quindi è prima di tutto un programmatore, cioè un esperto capace di scrivere il codice con cui sono costruiti i software. Lavora continuamente per migliorarli e renderli più accessibili a tutti (da questo deriva la radice etimologica della parola *hacker*: il verbo *to hack* significa "tagliare", "sfondare", aprirsi un varco tra le righe di codice che compongono un software).

Con il trascorrere del tempo, però, è emersa la figura dell'*hacker* che opera per un suo tornaconto personale. Molti *hacker* infatti utilizzano le loro abilità tecniche per identificare eventuali "buchi" nel sistema informatico delle organizzazioni o degli utenti che hanno preso di mira, in modo da mandare in crash il sistema stesso, o sottrarre dati e informazioni da utilizzare a proprio piacimento.

È così nata la distinzione tra l'*hacker etico*, che mette alla prova i sistemi di sicurezza informatici per verificarne i limiti e proporre soluzioni per migliorarli, e l'*hacker immorale*, che invece compie crimini informatici per un suo tornaconto.

### 1.1.4. Le linee guida e gli standard di sicurezza informatica

Sia in ambito professionale che aziendale è necessario osservare specifiche norme, che tutelano la sicurezza dei sistemi informatici e dei dati. È importante che queste norme vengano osservate da tutte le persone coinvolte nei processi aziendali.

A livello nazionale, l'istituto che si occupa di definire le linee guida, i regolamenti e gli standard in ambito digitale sia per la pubblica amministrazione che per le imprese è l'AGID (*Agenzia per l'Italia Digitale*). Per conoscere ogni aspetto dell'operato dell'AGID, è possibile consultare il sito *agid.gov.it*.

Oltre alle norme dell'AGID, esistono precisi standard di sicurezza informatica a cui gli enti pubblici e privati possono rifarsi per ridurre al minimo la quantità e la pericolosità delle minacce derivanti da Internet e dalla gestione di dati e informazioni digitali.

Lo standard ISO/27001 (*Tecnologia delle informazioni — Tecniche di sicurezza — Sistemi di gestione della sicurezza delle informazioni — Requisiti*) è una norma internazionale che definisce i requisiti per configurare un sistema con cui gestire la sicurezza delle informazioni, e include aspetti relativi alla sicurezza logica, fisica e organizzativa.

Ogni organizzazione, con l'assistenza di provider specializzati, può acquisire una certificazione di qualità che attesta l'allineamento del proprio sistema alle regole previste dallo standard.

## 1.2. Le principali misure di sicurezza online

Avendo compreso quali sono le minacce a cui sono esposti i nostri dispositivi, vediamo come possiamo difenderci.

### 1.2.1. L'autenticazione tramite nome utente e password

Per accedere a qualsiasi account (di posta elettronica, di una *home banking*, di *Facebook*, e così via), ci viene richiesto di autenticarci. Dobbiamo, cioè, farci riconoscere dal sistema, e inserire dunque la *password* da noi impostata quando abbiamo registrato l'account. Insieme alla password, molto spesso ci viene richiesto di digitare il *nome utente*.

Il nome utente svolge una funzione diversa rispetto alla password. Stabilisce infatti la nostra identità, ma non è un vero e proprio sistema di sicurezza. Nella maggior parte dei casi, infatti, il nome utente corrisponde al nome dell'utilizzatore del servizio o al suo indirizzo email. Pertanto non è un codice unico, stabilito per accedere al proprio account.

**Nota**. Il nome utente — che in inglese si pronuncia *User name* — è anche detto ID utente o User ID, o più semplicemente ID.

La procedura secondo cui dobbiamo inserire il codice utente e la password per accedere al nostro account si chiama *login*. Eseguire il login significa dunque fornire i dati necessari per riconoscere la nostra identità prima di accedere a una rete, a un sistema informatico o a un servizio online.

La procedura contraria invece si definisce *logout*, ed è importante eseguirla ogni volta che si esce dal proprio account. Il logout infatti determina la disconnessione dalla rete, dal sistema informatico o dal servizio online a cui ci eravamo collegati. Pertanto rappresenta un valido sistema di sicurezza per evitare che altre persone possano accedere alle nostre informazioni personali.

**Suggerimento**. Per scegliere le password sicure, osserva queste indicazioni:

- Utilizza combinazioni difficili da indovinare
- Non usare mai i tuoi dati anagrafici
- Utilizza password diverse per ognuno dei tuoi accessi (all'account di posta elettronica, al tuo account *Google*, al tuo profilo *Facebook*, *Istagram*, e così via)
- Componi password di almeno 8 caratteri
- Utilizza sia lettere maiuscole che minuscole, numeri e segni speciali (ad esempio, ! / ? _)
- Cambia le tue password di tanto in tanto (ogni due o tre mesi, ad esempio)

**Nota**. La *One-Time Password* (OTP) è una password valida solo per un accesso o una transazione. Se un hacker, quindi, riuscisse a intercettare una OTP appena utilizzata, non potrebbe più accedere ai dati protetti. È usata spesso nell'ambito delle transazioni bancarie: la OTP è generata da un dispositivo associato al login: ogni volta che l'utente deve accedere al servizio, crea una password usa e getta. Una volta che hai inserito correttamente username e password nel login (del tuo computer o della tua casella di posta elettronica, ad esempio), potrai autenticarti ed entrare nel sistema. Da questo momento, le tue attività sono tracciate e monitorate da parte di chi gestisce il sistema: questo monitoraggio si definisce *accountability*. (tracciabilità)

### 1.2.2. L'autenticazione a più fattori

L'autenticazione a più fattori è uno dei metodi più sicuri per proteggere qualsiasi account. Moltissimi siti e servizi online, come *Google*, *Facebook*, *Microsoft*, *Apple* offrono la possibilità di attivare l'autenticazione a due fattori.

Il suo funzionamento è molto semplice: per poter accedere al proprio account, oltre all'username e alla password, occorre inserire il PIN (un codice di sicurezza monouso, composto solitamente da 4 o 6 cifre) che ci viene spedito istantaneamente tramite SMS, email, o che possiamo trovare su un'apposita applicazione.

I metodi di autenticazione a più fattori sono due: *la doppia autenticazione tramite applicazione*, e la *One Botton Authentication*.

- **Doppia autenticazione tramite applicazione**. Esistono alcune applicazioni (come *Google Authenticator* o *Authy*) che hanno reso molto sicura l'autenticazione. Quando ci si iscrive a un nuovo servizio, è possibile creare un codice di sicurezza da condividere con lo smartphone attraverso un QR Code. Dopo aver scansionato il codice QR, sullo schermo del proprio smartphone, compare un nuovo PIN ogni trenta secondi. Ogni PIN resta valido ed è pertanto utilizzabile solo in questo brevissimo lasso di tempo. Questo metodo di autenticazione è sicuro perché non c'è nessun intermediario tra l'utente e il server: nessun provider, nessun operatore telefonico.
- **One Button Authentication**. È uno degli ultimi metodi realizzati per aumentare la sicurezza su Internet. Viene, però, supportato da pochissime piattaforme online. L'unica in Italia, al momento, è *Google*, che lo ha implementato in alcuni suoi servizi. Il funzionamento è molto semplice: basta premere il bottone *Sì, sono io* per poter accedere al proprio account. In questo caso, il codice per l'accesso viene riconosciuto automaticamente dal servizio e non c'è bisogno di inserirlo manualmente.

### 1.2.3. Riconoscimento dei dati biometrici

Gli smartphone più recenti sono muniti di speciali sensori con cui acquisire e riconoscere sia impronte digitali che dati biometrici, come quelli del proprio volto.

Questo sistema di riconoscimento attraverso le caratteristiche biometriche di una persona prende il nome di AIDC (*Automatic Identification and Data Capture*), e permette di rafforzare gli strumenti di sicurezza informatica.

Nei prossimi smartphone e notebook i sensori biometrici saranno sempre più usati proprio perché la sicurezza informatica sta diventando un requisito fondamentale per i dispositivi, e l'uso di password, da solo, non è più sufficiente.

Lo scanner per le impronte digitali, ad esempio, è molto diffuso sugli smartphone: l'accesso allo schermo e alle app è molto più sicuro rispetto all'uso dei metodi di sblocco, come il PIN o la password.

**Nota**. Con il termine "biometria" in informatica si intende un sistema in grado di riconoscere e identificare un individuo in base ad alcune caratteristiche fisiologiche. Si tratta di aspetti personali unici come iride, impronte digitali, retina, fisionomia, e così via. I dati biometrici sono dunque delle informazioni altamente riservate che un apparecchio registra per permettere all'utente di accedere al suo account o al suo dispositivo.

## 1.3. Le principali tecniche di violazione dei dati personali

I dati personali riguardano la sfera individuale delle persone fisiche. In base alle disposizioni del codice civile, le persone fisiche sono tutti gli individui a cui la legge attribuisce sia diritti che doveri.

Gli istituti pubblici e privati raccolgono dati personali, e sono pertanto tenuti a rispettare precise norme sulla loro conservazione, in modo da impedire a malintenzionati di utilizzarli per scopi illegali.

In Europa, la protezione dei dati personali è disciplinata dal GDPR (*General Data Protection Regulation*), ossia dal Regolamento (UE) 2016/679. A partire dal 24 maggio 2016, il GDPR ha sostituito la precedente fonte giuridica in materia di trattamento dei dati personali, ossia la Direttiva 95/46/CE del 24 ottobre 1995.

Ai sensi di quanto disposto dal GDPR, il dato personale è qualsiasi informazione che riguarda una persona fisica, come il nome, i dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

### 1.3.1. Le tecniche di ingegneria sociale

Sempre più hacker utilizzano sofisticate tecniche per trafugare dati e informazioni personali di ogni genere. Queste tecniche si definiscono di "ingegneria sociale" (*social engineering*), e sono a metà strada tra la psicologia e l'ingegneria.

L'ingegneria sociale è una manipolazione psicologica che induce chi ne è vittima a comportarsi in una determinata maniera o a rivelare informazioni personali senza rendersene realmente conto.

Si tratta di attività più articolate dei normali malware, ma possono portare a risultati molto più fruttuosi, in termini di acquisizione di notizie personali. È chiaro che queste tecniche possono essere utilizzate anche nei confronti, ad esempio, dei dipendenti di un'azienda per carpirne i segreti organizzativi e produttivi.

Esaminiamo dunque alcune tecniche di ingegneria sociale.

- Spacciandosi per un'altra persona, come ad esempio il gestore della connessione Internet, il pirata informatico chiama al telefono le sue potenziali vittime, e cerca di ottenere da loro le informazioni che gli consentiranno di perseguire i suoi scopi fraudolenti. In questo caso, il pirata informatico usa tecniche precise che possono consentirgli di conoscere i dati personali delle sue vittime. Ad esempio, può fingersi il delegato di un preciso istituto per conto del quale esegue sondaggi. Sono le persone più anziane o poco esperte ad essere le vittime preferite per questo tipo di reati.
- Un'altra tecnica di ingegneria sociale molto diffusa è il *phishing*. Questa tecnica fraudolenta si basa sull'invio di email ingannevoli. Di solito, il pirata informatico invia una email alla sua potenziale vittima, in cui la esorta a collegarsi a una specifica pagina web, e a inserire i suoi dati personali. Di solito i messaggi di queste email sono allarmanti. Possono ad esempio comunicare alla vittima che ci sono problemi con il suo conto bancario o con una sua spedizione, e che per risolverli sono necessari i suoi dati personali. Se la vittima della frode esegue le operazioni che gli vengono richieste nella email, il pirata informatico riesce a rubarle i dati, e in questo modo è in grado di utilizzarli per i suoi scopi fraudolenti.
- Lo *shoulder surfing* è la tecnica con cui il pirata informatico spia la sua potenziale vittima per rubarle i dati. Ad esempio, questa tecnica viene spesso utilizzata per duplicare il PIN durante le operazioni di prelievo da un bancomat, oppure per conoscere il PIN che la vittima utilizza per accedere al suo computer.

**Nota**. Si discute molto del lavoro che sembra stiano facendo i pubblicitari di grandi aziende: monitorando le nostre attività online, creano profili delle nostre preferenze, con cui organizzare campagne commerciali o offerte ad hoc. Questa tecnica si chiama *profilazione*, ed è il sistema più efficace per proporre contenuti mirati sul Web. Può sembrare una cosa buona e utile per tutti, ma si tratta di valutarne i pro e i contro per i cittadini. Il tema della tutela dei dati personali è molto dibattuto e complesso.

### 1.3.2. Difendersi dagli attacchi di ingegneria sociale

Qui di seguito, elenchiamo alcuni consigli per difenderti dagli attacchi di ingegneria sociale.

- Utilizza firewall, antivirus e antispyware per proteggere le tue transazioni online.
- Proteggi la tua connessione wireless domestica con una password.
- Mantieni aggiornati tutti i software (browser compreso) attraverso gli aggiornamenti automatici.
- Fai attenzione a offerte troppo vantaggiose, agli avvisi della banca che comunica l'immediata chiusura del tuo conto se non esegui azioni immediate, agli avvisi di vincita di lotteria o ai rifiuti di un incontro di persona per concludere una transazione. Lo scopo di questi messaggi è quello di spingerti a visitare un sito web fasullo, in cui i gestori possono carpire i tuoi dati.
- Tieni segreti password e PIN, e non inviarli mai per email o con messaggi istantanei.
- Utilizza password diverse per ognuno dei tuoi account. Se memorizzi sempre la stessa password per accedere a ogni tuo account, chiunque se ne impadronisca, può mettere a rischio tutte le tue informazioni sensibili.
- Digita tu stesso gli indirizzi dei siti web a cui vuoi accedere: se lo fai cliccando su collegamenti contenuti in messaggi in email, SMS o messaggi istantanei, potresti essere portato su siti legittimi solo in apparenza, per niente affidabili.
- Controlla gli indicatori di protezione delle informazioni dei siti che stai visitando. Se sei in un sito e-commerce e intendi fare un acquisto online, prima di immettere i tuoi dati, verifica che nella barra degli indirizzi, prima del nome del sito, ci sia la dicitura

*https* (la s sta per *secure*) e il logo del lucchetto chiuso. Sono indicatori che ti fanno capire che il sito è sicuro.

- Usa solo il tuo PC per fare ogni transazione finanziaria. Non pagare, non fare acquisti o altre attività finanziarie su computer pubblici o condivisi, oppure su dispositivi mobili come notebook o smartphone, che siano connessi a reti pubbliche wireless. La protezione, in questi casi, non è affidabile.
- Usa sempre il buon senso e se hai dubbi di qualsiasi tipo, prima di fare alcunché, chiedi informazioni ai tuoi genitori, al tuo docente o a un amico che ne sappia più di te.

### 1.3.3. Il furto di identità

Un'altra attività dell'ingegneria sociale è il furto di identità e, cioè, il furto di dati personali e sensibili a scopo di frode, un crimine che esiste da sempre, ma che l'avvento del Web ha riportato in auge. Le tecniche usate sono diverse, come diversi sono gli obiettivi di chi li mette in atto.

L'informatica e le nuove tecnologie hanno creato rischi fino a ieri impensabili, e ancora troppo poco conosciuti dai consumatori. A tutti coloro che usano Internet viene chiesto regolarmente di fornire informazioni personali per poter accedere a determinati siti o per poter acquistare beni e servizi. Queste informazioni viaggiano spesso in Rete in chiaro e non in modalità protetta.

Un crescente numero di utenti, inoltre, fornisce un'elevata quantità di dati personali a blog, siti di chat, social networks, e questo ha attratto molto l'attenzione degli hacker.

I dati personali hanno un mercato vastissimo e milionario: con essi si fabbricano documenti falsi, transazioni allo scopo di riciclaggio di denaro sporco, intestazioni di false polizze assicurative, contratti di finanziamento, e così via.

Ma vi è di più: soprattutto tra i più giovani, si diffonde il furto d'identità non inteso in senso strettamente economico, ma attuato attraverso l'appropriazione indebita di profili di social network utilizzati, ad esempio, per ledere l'immagine o la professionalità altrui.

### 1.3.4. Prevenire il furto di identità

Se ci informiamo, ci proteggiamo e gestiamo con attenzione i nostri dati, le possibilità di essere truffati diminuiscono. La prima regola è non sottovalutare la furbizia dei ladri d'identità. Se nel mondo reale possiamo riuscire a comprendere se qualcuno ci sta truffando, in quello virtuale è molto più difficile.

Per prevenire il furto di identità, segui queste semplici indicazioni:

- Proteggi il tuo PC con antivirus, firewall, antispamming, antiphishing, certificati digitali, patch.
- Gestisci con attenzione la posta elettronica.
- Non riutilizzare mai la stessa password per diversi account e modificale spesso.
- Non memorizzare PIN, password, nome utente o altri parametri per l'accesso ai servizi delle banche sullo smartphone.
- Non annotare password in nessun luogo, né cartaceo né elettronico, ma imparale a memoria.
- Utilizza con circospezione computer pubblici, come quelli nelle biblioteche.
- Visita siti il cui indirizzo inizi con il prefisso "https" con vicino il simbolo del lucchetto o di una chiave non rotta, e controlla sempre l'indirizzo, per esser certo che non si tratti di una copia.
- Salva i siti che visiti più spesso tra i preferiti e accedi da lì.

### 1.3.5. Capire se la propria identità è stata rubata

Quando sospetti di essere vittima di un furto di identità, segui queste indicazioni:

- Blocca le carte di credito e tutti i conti correnti interessati. La prudenza non è mai troppa: è meglio congelare tutto subito piuttosto che dover contestare, in seguito, eventuali acquisti fatti da un criminale informatico che ti ha rubato i dati.

- Comunica la cosa a tutti gli esercenti presso cui utilizzi regolarmente la tua carta, per segnalare che sono possibili eventuali usi fraudolenti. Dai seguito alla telefonata con una lettera raccomandata con ricevuta di ritorno.
- Modifica le password di tutti i tuoi account.

Se sei certo di essere una vittima di furto, segui queste indicazioni:

- Denuncia l'accaduto al Pronto Intervento (112 per i Carabinieri, 113 per la Polizia di Stato).
- Recati negli uffici dell'Autorità di Polizia Giudiziaria, e fai la tua denuncia, fornendo gli estremi dei documenti che sono stati sottratti.
- Se sospetti che qualcuno abbia usato il tuo nome o altre informazioni per effettuare un acquisto a credito o richiedere un prestito, contatta la tua banca per segnalare l'accaduto e valutare se sia necessario bloccare la carta.

Quando capita una cosa del genere, può passare anche un po' di tempo prima che tutto torni come prima: prendi nota di tutte le comunicazioni e rivolgiti a una associazione di difesa dei consumatori per ottenere consigli e consulenza su come agire per risolvere il problema e riconfermare, quando serve, la tua affidabilità creditizia. Le associazioni dei consumatori potranno fornirti anche tutela legale specialistica.

## 1.4. Misure per la sicurezza dei file

Ci sono specifiche misure di sicurezza che possiamo adottare per tenere al sicuro da potenziali minacce i nostri file.

### 1.4.1. Registrare ed eseguire una macro

Nelle applicazioni *Word* ed *Excel* della suite per ufficio *Microsoft Office*, le macro sono piccoli programmi scritti secondo il linguaggio VBA (*Visual Basic Applications*), con cui riprodurre un'intera sequenza di operazioni. Alle macro è possibile associare un comando, in modo che una volta selezionato, vengano automaticamente eseguite tutte le operazioni registrate insieme alla macro.

**Nota**. Facciamo un esempio: lavori in un'azienda e, alla fine di ogni mese, devi presentare al responsabile della contabilità un foglio elettronico di Excel con un report dei pagamenti ricevuti dai clienti. Potresti decidere di segnare di rosso e in grassetto tutti i clienti morosi: i clienti, cioè, che dovendo pagare entro la fine del mese, sono ancora insolventi. Potresti creare e eseguire una macro per applicare rapidamente queste modifiche di formattazione alle celle selezionate.

Nonostante le macro siano scritte nel linguaggio di programmazione *Visual Basic for Application*, non ci vogliono particolari competenze per utilizzarle. È sufficiente infatti avviare il registratore di macro, ed eseguire le operazioni da memorizzare.

In *Microsoft Word*, per avviare la registrazione di una macro, segui questa procedura:

1. Apri la scheda *Visualizza*, e nel gruppo comandi *Macro*, fai clic sulla freccia verso il basso, al di sotto del pulsante *Macro*.
2. Nel menu che si apre, seleziona l'opzione *Registra macro*.
3. Nella finestra di dialogo *Registra macro*, inserisci il nome che desideri assegnare alla tua macro. Cerca di scegliere il nome in base alla funzione della macro: ti sarà più facile riconoscerla quando ne avrai registrate più di una. Ricorda inoltre che il nome può contenere soltanto lettere, numeri e trattini bassi (_). Non puoi utilizzare né spazi né altri caratteri.
4. Scegli se eseguire la macro tramite un pulsante (che si aggiungerà a quelli già presenti nella barra di accesso rapido) oppure un comando da tastiera. Clicca su *Pulsante* per aprire la finestra di dialogo *Opzioni di Word*, e impostare il pulsante con cui eseguire la macro. Clicca invece sul pulsante *Tastiera* per aprire la finestra di dialogo in cui digitare la nuova combinazione con cui eseguire la macro.
5. Nella casella *Memorizza la macro in*, scegli se memorizzare la macro in tutti i documenti, oppure soltanto in quello corrente.
6. Fai clic sul pulsante *OK* per avviare la registrazione della macro.

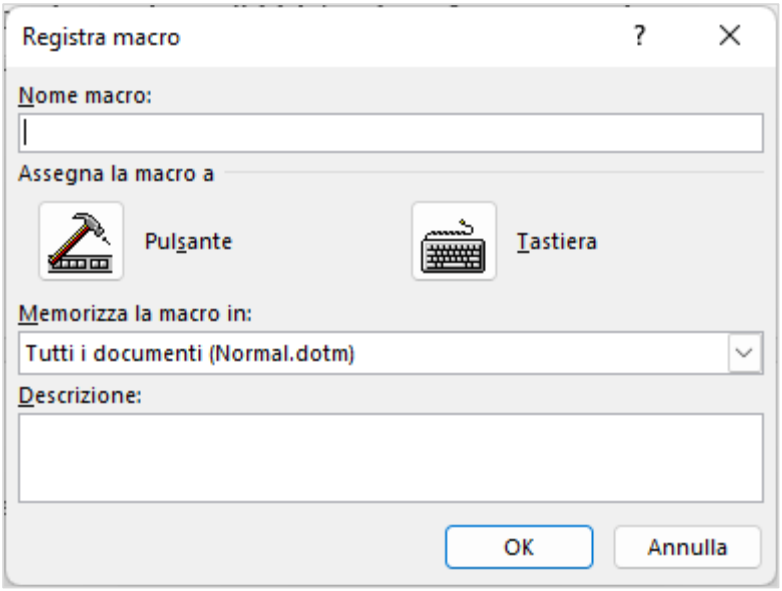



*Figura 1.1 — La finestra di dialogo di Word da cui avviare la registrazione di una macro*

7. Esegui le operazioni che desideri associare alla macro. Ad esempio, potresti digitare del testo e scegliere come formattarlo, oppure inserire immagini o altri oggetti grafici a cui associare complesse procedure di formattazione.

8. Per terminare la registrazione della macro, apri la scheda *Visualizza*, e nel gruppo comandi *Macro*, fai clic sulla freccia verso il basso, al di sotto del pulsante *Macro*. Nel menu che si apre, seleziona l'opzione *Interrompi registrazione*.

In *Microsoft Excel* la procedura per registrare una macro è simile a quella che hai appena visto:

1. Apri la scheda *Visualizza*, e nel gruppo comandi *Macro*, fai clic sulla freccia verso il basso, al di sotto del pulsante *Macro*.

2. Nel menu che si apre, seleziona l'opzione *Registra macro*.

3. Nella finestra di dialogo *Registra macro*, inserisci il nome che desideri assegnare alla tua macro.

4. Scegli la combinazione di tasti per avviare velocemente la macro. Nella casella *Tasto di scelta rapida*, inserisci il pulsante da premere insieme al tasto *CTRL*, affinché Excel esegua la macro. La combinazione è del tipo *CTRL + lettera*.

5. Fai clic sul pulsante *OK* per avviare la registrazione della macro.

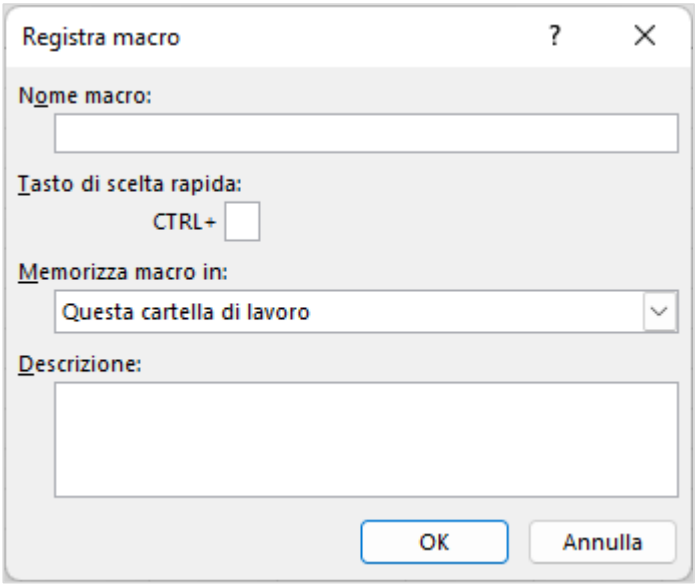



*Figura 1.2 — La finestra di dialogo di Excel da cui avviare la registrazione di una macro*

6. Esegui le operazioni che desideri associare alla macro.

7. Per terminare la registrazione della macro, apri la scheda *Visualizza*, e nel gruppo comandi *Macro*, fai clic sulla freccia verso il basso, al di sotto del pulsante *Macro*. Nel menu che si apre, seleziona l'opzione *Interrompi registrazione*.

La procedura per eseguire una macro è identica sia in *Word* che in *Excel*:

1. Nella barra multifunzione di *Word* o di *Excel*, apri la scheda *Visualizza*, e nel gruppo comandi *Macro*, seleziona il pulsante *Macro*.

2. Nella finestra di dialogo che si apre, trovi le macro da te registrate. Seleziona dunque la macro che desideri utilizzare, quindi fai clic sul pulsante *Esegui*.

### 1.4.2. Cambiare le impostazioni delle macro

Molte macro vengono create da sviluppatori di software, e sono pertanto già disponibili. Alcune macro tuttavia possono costituire un possibile rischio di sicurezza: un utente malintenzionato, un hacker, potrebbe inserire in un file (un documento di *Word*, ad esempio) una macro capace di diffondere un virus nel computer o nella Rete, e inviarla in allegato a una email. Per evitare possibili infezioni, sarebbe meglio disattivare tutte le

macro contenute in un file di *Word* o di *Excel*. In questo modo, possiamo decidere se attivarle o meno.

La procedura per modificare le impostazioni iniziali delle macro è sostanzialmente la stessa sia in *Word* che in *Excel*:

1. Apri la scheda *File*, e nel menu a sinistra, seleziona la voce *Opzioni*.
2. Nel menu a sinistra della finestra di dialogo che si è appena aperta, seleziona la voce *Centro protezione*.
3. Seleziona il pulsante *Impostazioni Centro Protezione*.
4. Nel menu a sinistra della nuova finestra di dialogo, seleziona la voce *Impostazioni delle macro*.
5. Scegli una tra le opzioni disponibili:
    - *Disabilita le macro senza notifica*. Le macro e i relativi avvisi di sicurezza vengono disabilitati.
    - *Disabilita tutte le macro con notifica*. Le macro vengono disabilitate, ma ogni volta che ce n'è una, visualizzi un avviso, per cui puoi scegliere se attivarla o meno.
    - *Disabilità tutte le macro tranne quelle con firma digitale*. Disabilita tutte le macro, ma quando ce n'è una, visualizzi un avviso. Tuttavia, se la macro riporta la firma digitale di un autore attendibile viene eseguita automaticamente.
    - *Abilita tutte le macro.* Sarebbe meglio evitare di selezionare questa opzione, visto che esegue automaticamente tutte le macro contenute nei file quando vengono aperte, e pertanto espone il computer all'attacco potenzialmente dannoso.

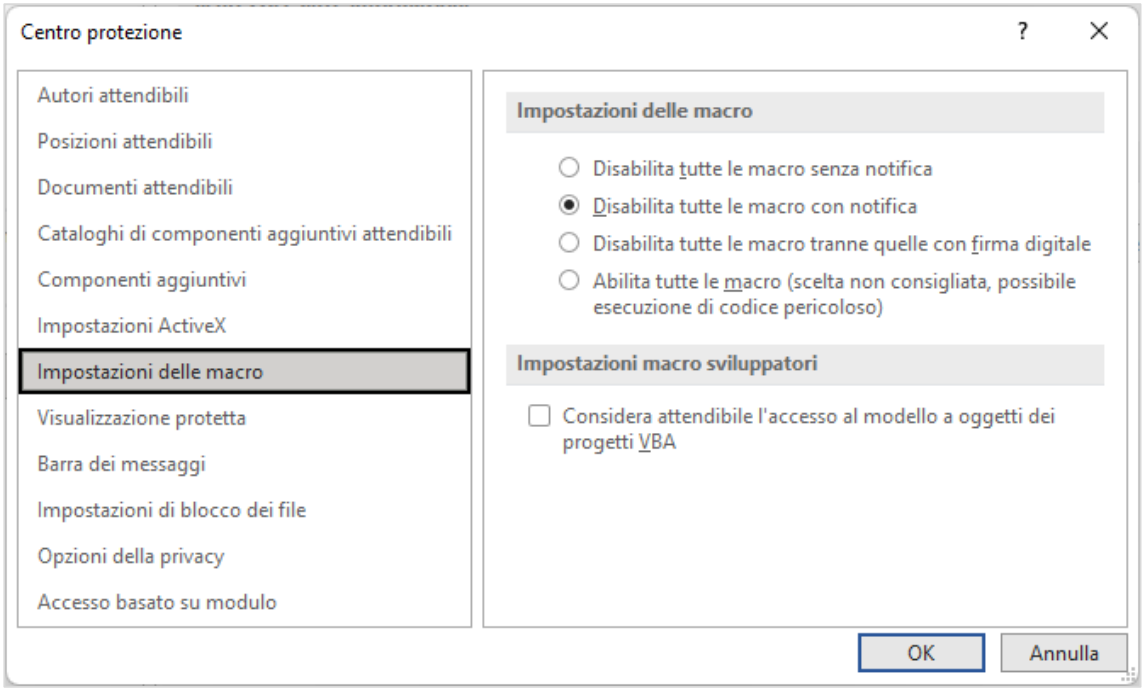



*Figura 1.3 — La finestra di dialogo di Word da cui modificare le impostazioni delle macro*

### 1.4.3. Proteggere i file con una password

Un modo sicuro per impedire a terzi di accedere ai tuoi documenti è impostare una password con cui aprirli. In *Microsoft Word*, per proteggere il documento corrente con una password, esegui questi passaggi:

1. Apri la scheda *File*, e nel menu a sinistra, seleziona l'opzione *Informazioni*.
2. Fai clic su *Proteggi documento*, e nel menu che si apre, seleziona l'opzione *Crittografia con password*.

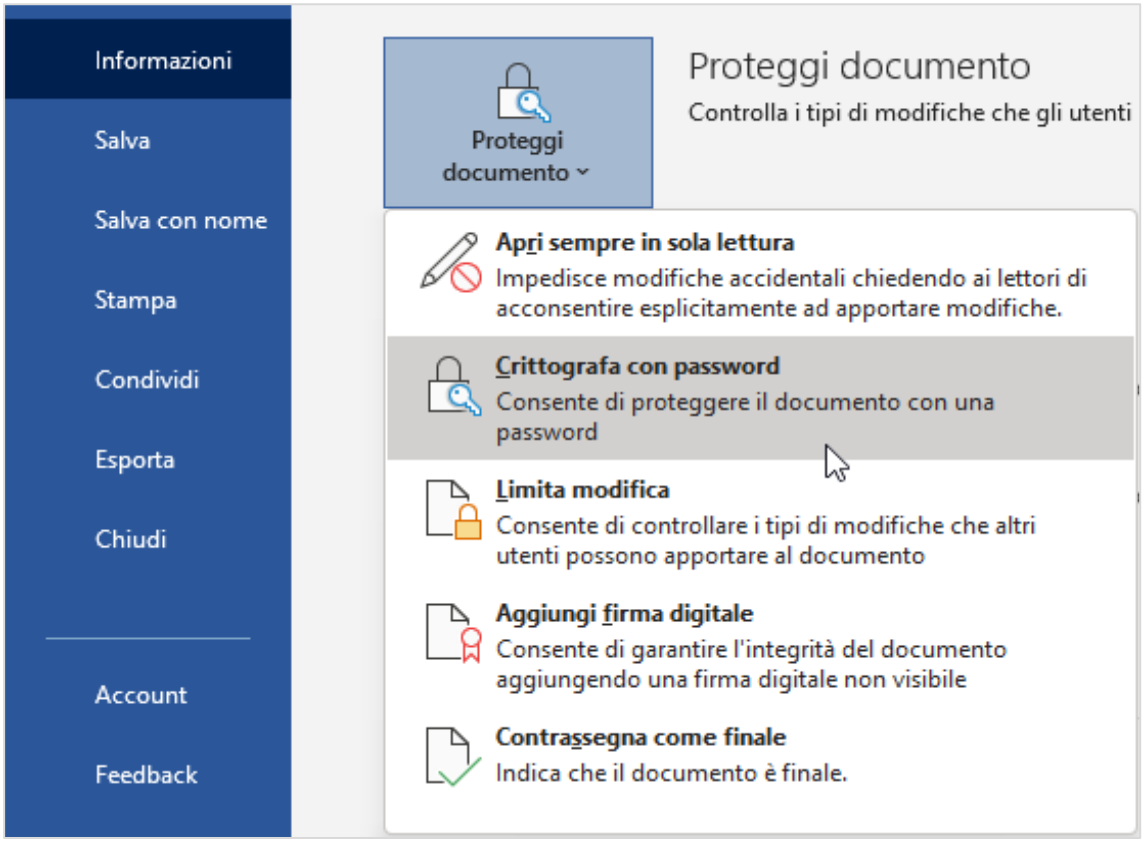



*Figura 1.4 — Inserire una password con cui proteggere un documento di Word*

3. Nella finestra di dialogo che si apre, inserisci la password da inserire per aprire il documento, e poi fai clic sul pulsante *OK*.

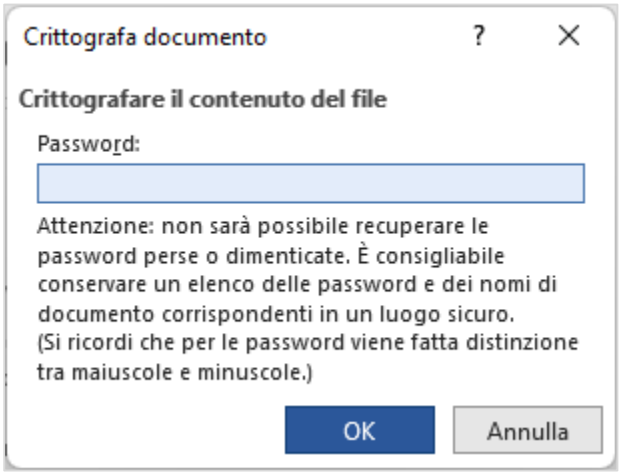



*Figura 1.5 — La finestra di dialogo di Word in cui inserire la password con cui proteggere un documento*

4. Inserisci nuovamente la password, e poi fai clic sul pulsante *OK*.

5. Apri la scheda *File*, e nel menu a sinistra, seleziona l'opzione *Salva*. In alternativa, puoi fare clic sull'icona a forma di floppy disc al di sopra della barra multifunzione di *Word*.

Da questo momento in poi, chiunque voglia accede al documento dovrà inserire la password da te impostata.

Per eliminare la password, esegui i passaggi che abbiamo visto fin qui, lasciando però vuota la casella in cui inserire la password (vedi la Figura 1.5).

Come vedrai nel modulo dedicato a *Excel*, le cartelle di lavoro sono i file in cui puoi inserire più fogli elettronici. Un modo sicuro per impedire a terzi di accedere alle tue cartelle di lavoro è impostare una password con cui aprirle.

In *Excel*, la procedura per proteggere la tua cartella di lavoro corrente con una password è simile a quella che abbiamo visto per Word.

1. Apri la scheda *File*, quindi seleziona *Informazioni* > *Proteggi cartella di lavoro* > *Crittografia con password*.
2. Nella finestra di dialogo che si apre, inserisci la password, quindi fai clic sul pulsante *OK*.
3. Conferma nuovamente la password, e poi fai clic su *OK*.

# 2. Attacchi e minacce informatiche

## 2.1. I diversi tipi di malware

L'espressione "malware" deriva dalla contrazione delle parole inglesi *malicious* (dannoso) e *software* (programma). Significa pertanto "programma dannoso".

Indica un qualsiasi programma creato allo scopo di causare danni al dispositivo su cui viene eseguito, e ai dati immagazzinati al suo interno. Alcuni malware invece vogliono accedere segretamente nei dispositivi per sottrarre le informazioni personali in essi racchiuse.

Generalmente i malware utilizzano Internet per diffondersi, ma possono anche provenire da email infette. In alcune occasioni invece possono provenire dai siti web visitati durante la navigazione in Internet. Anche le versioni di prova o gratuite di alcune applicazioni scaricabili da Internet possono contenere malware.

Nel momento in cui un qualsiasi dispositivo si connette a Internet è sottoposto al rischio di contrarre un malware. Come vedremo più avanti, ci sono più strumenti a cui ricorrere per difendere sistemi, dati e dispositivi, dalle minacce informatiche.

### 2.1.1. Virus informatici, Trojan e Worm

I *virus informatici* sono piccoli programmi o sezioni di codice, che contengono una sequenza di istruzioni in grado di attivare automaticamente azioni che danneggiano i computer.

Sono pericolosi per la loro capacità di duplicarsi. Parte delle istruzioni con cui sono stati programmati infatti impongono loro di creare copie di sé stessi.

Agiscono inoltre in maniera simile ai virus biologici. Possono infatti diffondersi da un dispositivo all'altro, e innescare un contagio simile a quello creato dalle epidemie.

Di solito i virus informatici si nascondono all'interno di altri programmi, ed entrano in funzione dopo aver eseguito questi programmi. Richiedono dunque l'intervento umano per attaccare. Un sistema molto usato per diffondere i virus è la posta elettronica. I programmi che contengono i virus possono infatti essere allegati alle email.

In generale, i virus danneggiano il software dei dispositivi che li ospitano. A volte però possono provocare danni anche all'hardware, e causare ad esempio il surriscaldamento della CPU, o il blocco della ventola di raffreddamento.

Anche quando non sono direttamente dannosi per il sistema operativo dei dispositivi, i virus informatici comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. I computer infettati da virus sono perfino in grado di agire autonomamente, ed eseguire operazioni senza che ce ne accorgiamo.

Come i virus, anche i *trojan* sono programmi capaci di infettare i dispositivi su cui vengono eseguiti. Si nascondono all'interno di altri programmi, in file audio, video, o tra gli allegati di una email che ci sembra innocua.

Lo scopo dei trojan è rubare informazioni personali, come password, numeri di carte di credito, o altri codici, e inviarle agli hacker. Alcuni trojan invece permettono agli hacker di utilizzare Internet per prendere il controllo dei dispositivi, in modo da copiare, modificare e cancellare i dati al loro interno. I trojan infatti contengono programmi dannosi, che entrano nei nostri sistemi per infettarli senza che ce ne accorgiamo.

I *worm* (letteralmente traducibile con la parola "verme"), dopo essersi infiltrati in un computer, sono in grado di replicarsi, e infettare altri dispositivi.

Una volta entrati in un dispositivo, i worm ricercano gli indirizzi email nei programmi di posta elettronica, e li utilizzano per inviare email a cui allegano file infetti, che contengono delle loro copie. Quando i destinatari delle email aprono questi file, i worm entrano in azione, e continuano a replicarsi.

Le email inviate automaticamente dai worm contengono messaggi che sfruttano tecniche di ingegneria sociale per convincere i destinatari ad aprire il file infetto, allegato alle email.

Lo scopo dei worm è creare malfunzionamenti del dispositivo in cui sono riusciti a entrare, e attivare dunque operazioni inutili e dannose.

### 2.1.2. Spyware, adware e ransomware

Gli *spyware* sono piccoli programmi, che si installano automaticamente sui nostri dispositivi, quando raggiungiamo siti web che possono infettarci. In altre occasioni, siamo

noi a installarli sui nostri dispositivi in modo involontario. Ciò accade soprattutto quando scegliamo di utilizzare programmi gratuiti, che in realtà contengono spyware.

Gli spyware vengono utilizzati dagli hacker per acquisire più informazioni possibili sulle nostre abitudini di navigazione, sulla cronologia dei siti da noi visitati, e sui nostri dati personali (come i numeri delle carte di credito, che utilizziamo per eseguire i pagamenti online).

Queste informazioni vengono successivamente vendute a società commerciali, che in questo modo possono conoscere le nostre preferenze, e inviarci email pubblicitarie mirate (è questa in parte l'origine del così detto *spam*, di cui abbiamo parlato nel secondo modulo).

Gran parte delle persone non riesce a rendersi conto quando il proprio dispositivo è infetto da spyware, a causa della sua capacità di nascondersi. Tuttavia, quando uno spyware entra in funzione, si attivano operazioni che, altrimenti, non si attiverebbero mai. Ne elenchiamo alcune.

- Mentre lavoriamo, compaiono in continuazione pop-up pubblicitari. I pop-up sono finestre che compaiono automaticamente sugli schermi dei nostri computer per comunicarci alcune informazioni o per mostrarci dei messaggi precisi. I pop-up di solito sono fastidiosi perché occupano gran parte dello schermo, ma a volte sono indispensabili per navigare correttamente sui siti web.
- Nelle nostre applicazioni o nel nostro sistema, vengono automaticamente modificate impostazioni che siamo certi di non aver cambiato personalmente, e che non riusciamo a resettare. L'esempio più classico è la modifica della pagina iniziale del nostro browser. Anche ripristinando la nostra pagina iniziale, a ogni riavvio torna quella indesiderata.
- Il nostro browser contiene componenti aggiuntivi che non ricordiamo di aver scaricato. Succede spesso, ad esempio, che compaiano barre degli strumenti che non ci servono o non desideriamo, e che ricompaiono a ogni riavvio del computer anche se le abbiamo eliminate.
- Il computer è lento. I malware infatti non devono garantire migliori prestazioni tecniche dei dispositivi che li ospitano. Le risorse che utilizzano per monitorare le

nostre attività e inviare pubblicità possono rallentare il computer e provocare errori del sistema operativo, senza che ciò sia un problema.

Gli *adware* sono forse il tipo di infezione informatica più fastidiosa. Sono infatti software dannosi che mostrano sullo schermo del computer infetto una serie continua di finestre pop-up con annunci pubblicitari, e anche se tentiamo di chiuderle, le finestre ricompaiono.

Come gli spyware, anche gli adware si nascondono all'interno di programmi scaricabili gratuitamente da Internet.

I *ransomware* sono una grave forma di minaccia. Riescono infatti a bloccare i dispositivi una volta infettati, in modo che gli hacker possano chiedere alle loro vittime un riscatto in denaro per tornare a fare funzionare i dispositivi.

Se gli hacker sono in grado di impiegare ransomware per bloccare qualsiasi dispositivo, significa che sono anche in grado di copiare i dati nei dispositivi infettati, prima di ricevere il riscatto. Soddisfare le richieste degli hacker pertanto non ci dà alcuna sicurezza che i nostri dati siano al sicuro, e che non siano stati violati.

I ransomware possono infiltrarsi in un qualsiasi dispositivo attraverso un allegato a una email infetta, o dopo aver aperto un sito infetto, attraverso il browser.

### 2.1.3. Rootkit, backdoor e keylogger

I *rootkit* sono una categoria di malware che funziona in modo simile ai trojan. Sono infatti programmi con cui gli hacker possono controllare i nostri dispositivi senza che ce ne rendiamo conto, in qualità di amministratori del sistema.

Le *backdoor* sono malware con cui gli hacker possono aggirare i sistemi di sicurezza dei nostri dispositivi per controllarli dall'esterno (da remoto). Le *backdoor* vengono impiegate anche per scopi leciti, come consentire a tecnici specializzati di compiere da remoto la manutenzione dei sistemi informatici.

I *keylogger* sono sistemi con cui intercettare tutto ciò che un utente digita sulla sua tastiera. Possono essere di due tipi: *hardware* o *software*. I primi vengono collegati al cavo di comunicazione tra la tastiera e il computer o all'interno della tastiera. Sono molto utili per appropriarsi indebitamente dei dati digitati sulle tastiere degli sportelli bancomat. I

secondi sono programmi con cui controllare e salvare la sequenza di tasti digitata da un utente su qualsiasi dispositivo.

### 2.1.4. Phishing, smishing, vishing, pharming e sniffing

Il *phishing* è una tecnica fraudolenta con cui gli hacker inviano alle loro potenziali vittime una email con alcuni campi da compilare o link a cui collegarsi. In questo caso, l'intento degli hacker è carpire i dati che le vittime dell'inganno inseriscono per rispondere alla email o di farle connettere a specifici siti, per poi sottrarre loro alcuni dati personali. Il phishing ovviamente utilizza tecniche di ingegneria sociale per spingere i destinatari delle email fraudolente a completare i campi della email o a cliccare sui link.

Quando il *phishing* avviene tramite messaggi (SMS o altri servizi di messaggistica, come *WhatsApp*) prende il nome di *smishing*. La parola *smishing*, infatti, è la combinazione di "SMS" (messaggi di testo) e "phishing" (il furto dei dati personali tramite messaggi fraudolenti). I messaggi fraudolenti, in questo caso, si inseriscono all'interno di una chat che la vittima ha già avuto con un altro soggetto, come una banca.

Il *vishing* è l'evoluzione del *phishing*. È legato all'utilizzo dei servizi VoID, con cui eseguire telefonate tramite Internet. Può succedere che il malintenzionato si spacci per una banca, facendo addirittura comparire il vero numero dell'istituto di credito sul display della sua vittima, spingendola così a comunicare i propri dati di accesso per risolvere fantomatici problemi o rendere di nuovo sicuro il proprio account.

Il *pharming* consiste nel riprodurre un sito web ufficiale, in modo che il mal capitato inserisca i suoi dati tranquillamente. Anche questa è un'evoluzione del *phishing*.

Lo *sniffing* è l'attività di intercettazione passiva dei dati che transitano in una rete telematica, attraverso software specifici detti, appunto, *sniffer*. Può essere utilizzata in modo fraudolento per intercettare informazioni sensibili, come login e password di accesso a un determinato servizio online.

## 2.2. Gli strumenti per difendersi dai malware

Ogni giorno compaiono nuovi malware, che possono infettare i nostri dispositivi o violarne la sicurezza. Internet è diventato il principale mezzo di trasmissione di ogni tipo di software infetto. Alcune volte, un semplice allegato a una email che abbiamo ricevuto da una mittente che ci sembrava attendibile può contenere una minaccia, altre volte invece ci siamo imbattuti in siti poco affidabili, e così facendo ci siamo esposti a una minaccia informatica.

Detto ciò, è indispensabile utilizzare dei sistemi che possano difendere i nostri dispositivi e i nostri dati dalle potenziali infezioni a cui sono sottoposti continuamente. Il principale di questi sistemi è l'antivirus.

### 2.2.1. Utilizzare un antivirus

Gli *antivirus* sono specifici programmi con cui possiamo rilevare ed eventualmente eliminare i malware che insidiano la sicurezza dei nostri dispositivi. Ciascun malware, infatti, è identificabile tramite una «firma», ossia una precisa stringa di codice che lo contraddistingue. Per riconoscere la minaccia, l'antivirus passa al setaccio i file all'interno del computer. In pratica, confronta tutto ciò che è in funzione sul computer con la propria banca dati, in cui vengono raccolte le *firme* dei nuovi malware che costantemente vengono distribuiti in tutto il mondo attraverso Internet.

Se l'antivirus trova in un file del computer una di queste firme, blocca il file, e ci segnala subito la cosa con un avviso. A questo punto, possiamo decidere di compiere più azioni:

- eliminare il file infetto;
- continuare a utilizzare il file anche se infetto;
- mettere il file infetto in quarantena, in modo che non possa più nuocere ("quarantena" è il nome di una cartella separata dal resto del sistema, in cui l'antivirus isola i file infetti).

In commercio, esistono molti antivirus, ciascuno con funzioni specifiche, e in grado di rilevare infezioni di tipo diverso. La maggior parte degli antivirus sono disponibili anche

gratuitamente. Le versioni gratuite degli antivirus tuttavia hanno funzioni ridotte rispetto alle versioni a pagamento.

Il sistema operativo *Windows* incorpora già un antivirus, il cui nome è *Defender*. Salvo esigenze particolari, gli utenti di *Windows* possono utilizzare questo antivirus per proteggere il proprio computer dalle minacce informatiche, senza doversene procurare un altro, gratuitamente o a pagamento.

**Nota**. Per eliminare spyware, adware e keylogger, bisogna utilizzare applicazioni specifiche, denominate *Antispyware*. In Internet è possibile trovarne di gratuite. Non tutti gli antivirus infatti eliminano spyware, adware e keylogger, visto che non sono dei veri e propri virus.

**Attenzione**. Sullo stesso dispositivo non possono funzionare più antivirus contemporaneamente.

### 2.2.2. Avviare una scansione del sistema con Windows Defender

Di solito gli antivirus entrano in funzione automaticamente, dopo aver acceso il dispositivo sul quale sono installati, ed eseguono un monitoraggio continuo del sistema (*real-time*). In pratica, analizzano istantaneamente le operazioni che il sistema esegue, e comprendono se si svolgono in maniera corretta o in modo allarmante. Così facendo, gli antivirus sono in grado di segnalare immediatamente la presenza di software infetto.

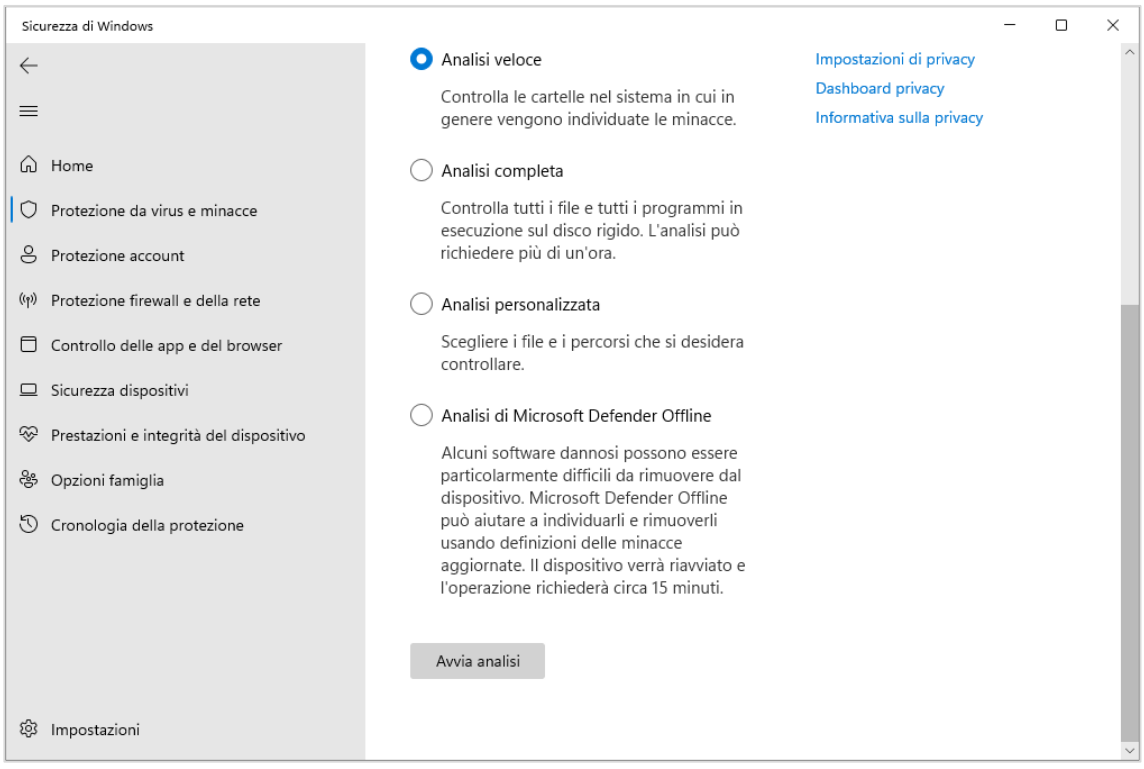
Oltre al monitoraggio continuo, possiamo utilizzare l'antivirus per scansionare in qualsiasi momento specifiche unità, cartelle o file. Quando riceviamo una email con allegato un documento o un file, anziché aprire subito l'allegato, sarebbe meglio scansionarlo con l'antivirus, in modo da verificare se contiene malware. Allo stesso modo, prima di eseguire i file che abbiamo scaricato da Internet, sarebbe meglio scansionarli con l'antivirus per controllare se al loro interno è nascosta un'applicazione dannosa.

La *scansione* dunque è il processo con cui un antivirus verifica la presenza di malware su qualsiasi sistema, unità o dispositivo.

Come abbiamo detto poco prima, gli antivirus oltre a proteggere costantemente i nostri dispositivi dagli attacchi informatici possono eseguire scansioni del sistema per rilevare la presenza di malware.

In *Windows 11* per avviare una scansione con l'antivirus *Defender*, segui questi passaggi:

1. Nella barra delle applicazioni, seleziona il pulsante *Start*, quindi fai clic su *Impostazioni*.
2. Nel menu a sinistra della finestra *Impostazioni*, seleziona *Privacy e sicurezza* > *Sicurezza di Windows* > *Protezione da virus e minacce*.
3. Nella finestra di dialogo *Sicurezza di Windows*, seleziona il pulsante *Opzioni di analisi*.
4. Scegli il tipo di analisi da eseguire: veloce, completa, personalizzata o Offline. L'*analisi veloce* controlla soltanto le cartelle del sistema in cui in genere vengono individuate le minacce, e pertanto richiede poco tempo. L'*analisi completa* controlla tutti i file e tutti i programmi in esecuzione sul disco rigido, e pertanto richiede molto tempo (in genere più di un'ora). L'*analisi personalizzata* ti permette di scegliere i file e i percorsi da controllare. L'*analisi di Microsoft Defender Offline* può essere una buona soluzione per ricercare i software particolarmente difficili da rimuovere dal dispositivo.
5. Dopo aver scelto il tipo di analisi da eseguire, seleziona il pulsante *Avvia analisi*.




*2.1 — La finestra di dialogo Sicurezza di Windows*

Una volta avviata la scansione, compare una barra di avanzamento che indica la sua percentuale di completamento, e il tempo necessario per completarla.

### 2.2.3. Accedere alla cronologia della protezione con Windows Defender

Se l'antivirus ha rilevato software dannosi, alla fine della scansione mostra un elenco con i malware rilevati, e i relativi livelli di rischio.

A questo punto, possiamo mettere in quarantena i file infetti (saranno cioè isolati in una cartella del computer creata dall'antivirus, in modo che non possono nuocere), o al contrario possiamo rimuoverli in maniera permanente, senza metterli in quarantena.

**Attenzione**. L'antivirus mette in quarantena i file che non è in grado di disinfettare, in attesa che la sua casa produttrice rilasci gli aggiornamenti con cui eliminare quel tipo di file.

Un'altra possibilità nel caso in cui l'antivirus rilevi software dannosi è quella di consentirli nel dispositivo, e quindi ripristinarli. In questo caso, però, occorre prestare molta attenzione ai file che decidiamo di ripristinare nonostante l'antivirus li segnali come infetti. Questa possibilità è da prendere in considerazione soltanto quando siamo sicuri che l'antivirus abbia inviato una segnalazione errata.

Per accedere alla cartella con i file messi in quarantena da *Windows Defender*, segui questi passaggi:

1. Nella barra delle applicazioni di *Windows 11*, seleziona il pulsante *Start*  , quindi fai clic su *Impostazioni*  .
2. Nel menu a sinistra della finestra *Impostazioni*, seleziona Privacy e sicurezza > Sicurezza di Windows > Protezione da virus e minacce.
3. Nella finestra di dialogo *Sicurezza di Windows*, seleziona il *pulsante Cronologia della protezione*.

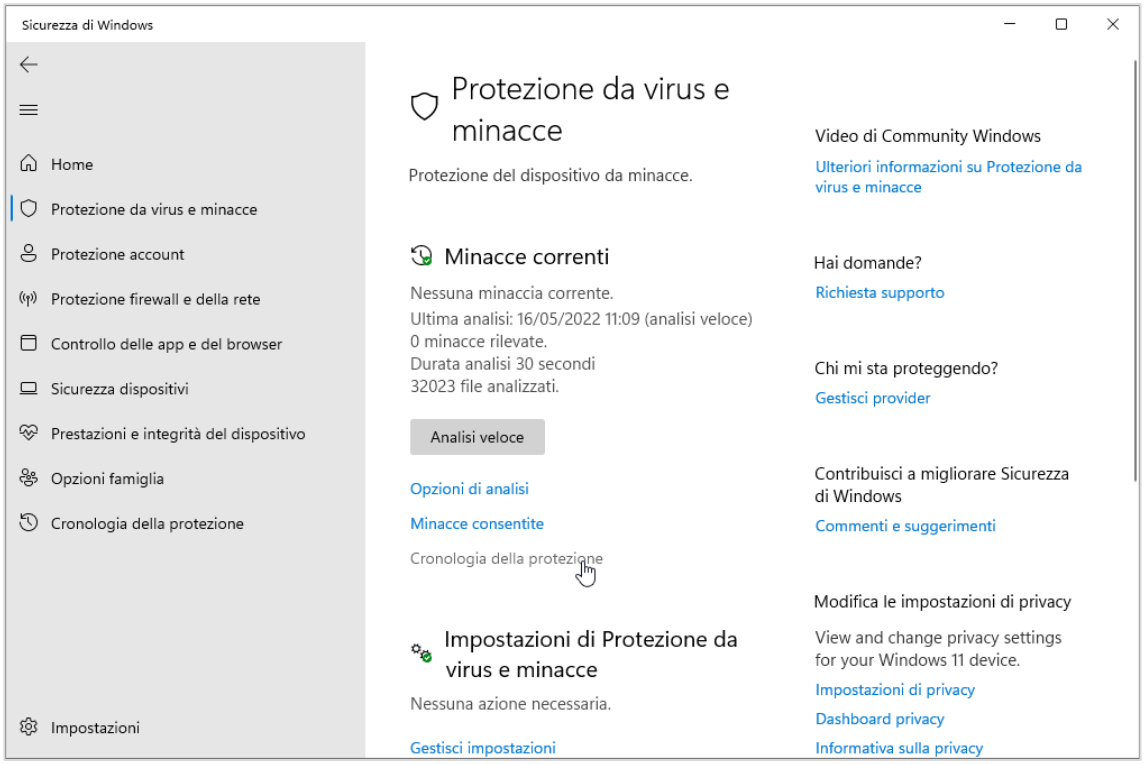



*Figura 2.2 — Accedere alla cronologia della protezione con Windows Defender*

A questo punto, compare l'elenco dei file infetti o sospetti che *Windows Defender* ha rilevato durante le scansioni precedenti. Puoi così decidere di rimuoverli definitivamente dal computer, oppure ripristinarli.

### 2.2.4. Pianificare la scansione del sistema con Windows Defender

Anziché avviare una scansione manualmente, possiamo programmarne l'esecuzione, in modo che avvenga in modo automatico nel momento in cui lo vogliamo.

In *Windows 11* per pianificare la scansione del sistema con l'antivirus *Defender*, segui questi passaggi:

1. Nella barra delle applicazioni, seleziona il pulsante *Start*, e nella casella di ricerca, digita *Utilità di pianificazione*.
2. Fai clic sul pulsante *Apri*.

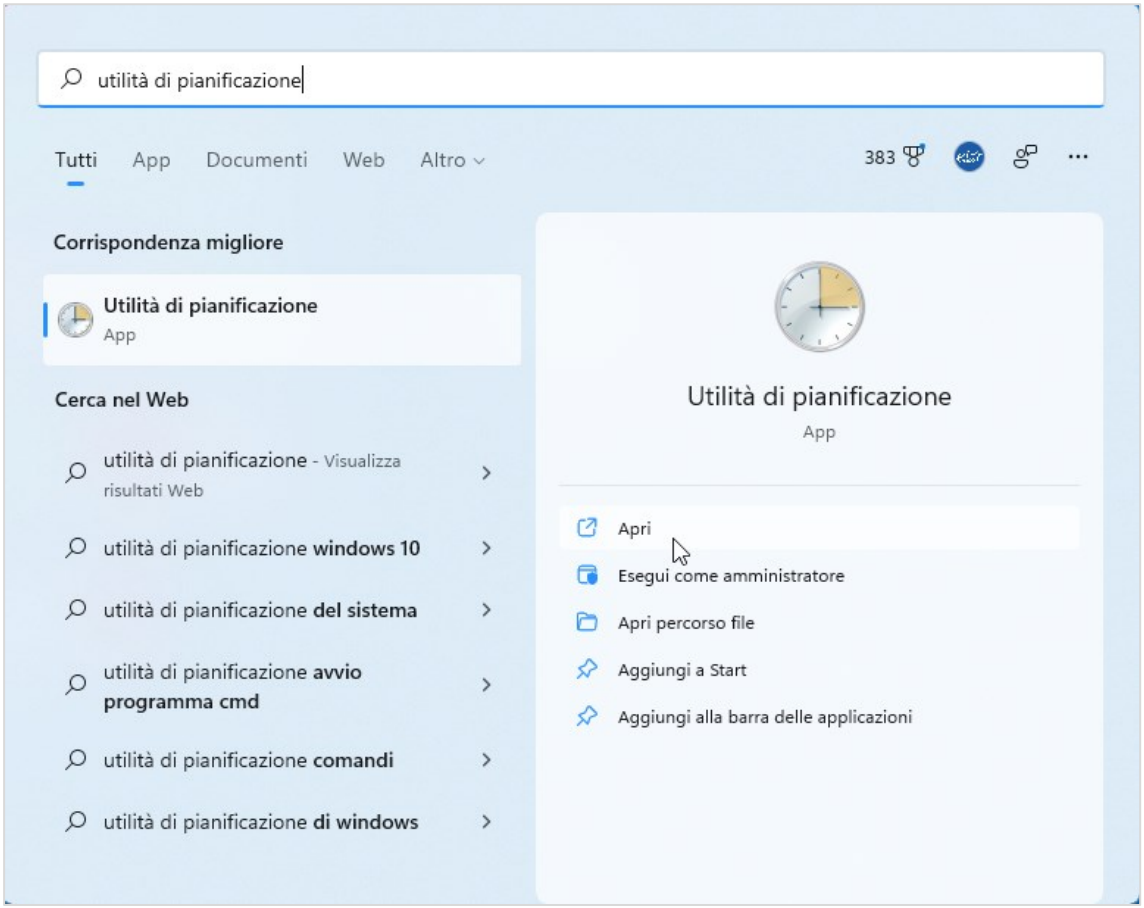



*Figura 2.3 — Aprire la finestra Utilità di pianificazione di Windows 11*

3. Nel menu a sinistra della finestra *Utilità di pianificazione*, fai clic sulla piccola freccia a sinistra della cartella *Libreria Utilità di pianificazione*, quindi seleziona *Microsoft* > *Windows* > *Windows Defender*.

4. Nel menu a destra della finestra *Utilità di pianificazione*, seleziona l'opzione *Crea attività*.

5. Nella finestra di dialogo *Crea attività*, apri la scheda *Attivazione*, e fai clic sul pulsante *Nuovo*.

6. Nella finestra di dialogo *Nuova attivazione*, trovi i comandi per pianificare la scansione del sistema con *Windows Defender*. Puoi ad esempio decidere di avviare la scansione giornalmente, settimanalmente, oppure mensilmente. Puoi inoltre scegliere il giorno e l'orario in cui avviarla.

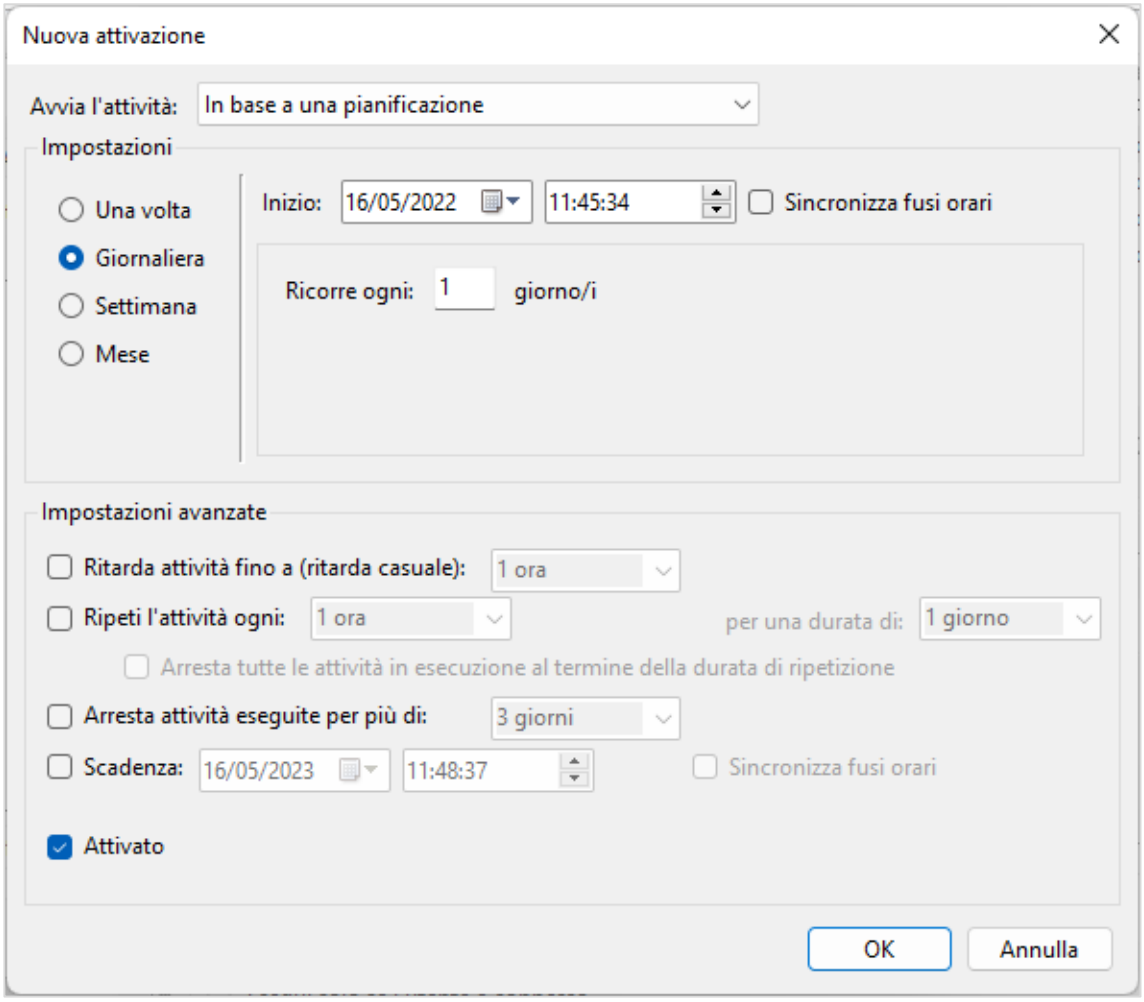



*Figura 2.4 — La finestra di dialogo di Windows 11 da cui pianificare la scansione del sistema con Defender*

### 2.2.5. Verificare la disponibilità di aggiornamenti per Windows Defender

Una tra le cose più importanti, è aggiornare costantemente l'antivirus. Come abbiamo già detto, ogni giorno compaiono nuovi tipi di malware, che vengono distribuiti in tutto il mondo attraverso Internet. Gli sviluppatori degli antivirus pertanto cercano di trovare costantemente soluzioni tecniche con cui bloccare i nuovi malware, e una volta trovate, inseriscono nelle banche dati dell'antivirus le nuove istruzioni e modifiche per combatterli.

L'aggiornamento del database dell'antivirus avviene, di solito, in base alle segnalazioni degli utenti o di gruppi specializzati che, per mestiere o per hobby, individuano nuovi malware. Sono infatti diverse le organizzazioni gestite e finanziate generalmente da università o enti governativi, che si occupano di raccogliere e rendere pubbliche le

segnalazioni di vulnerabilità o attacchi, al fine di aggiornare continuamente i registri delle firme dei malware.

Queste organizzazioni sono note con l'acronimo di CERT (*Computer Emergency Response Team*, ossia "Squadra di risposta alle emergenze informatiche").

Aggiornare l'antivirus permette dunque di proteggere le nostre informazioni personali dalle possibili minacce informatiche che frequentemente vengono diffuse.

Di solito, gli antivirus sono impostati per scaricare i loro aggiornamenti da Internet appena sono disponibili, e per installarli automaticamente. Tuttavia, anziché affidarsi a un sistema automatico, possiamo collegarci periodicamente con il sito web della casa produttrice dell'antivirus, e controllare se ci sono nuovi aggiornamenti da scaricare e installare.

In *Windows 11*, per verificare la disponibilità di aggiornamenti per l'antivirus *Defender*, segui questi passaggi:

1. Nella barra delle applicazioni, seleziona il pulsante *Start*  , quindi fai clic su *Impostazioni*  .
2. Nel menu a sinistra della finestra *Impostazioni*, seleziona *Privacy e sicurezza* > *Sicurezza di Windows* > *Protezione da virus e minacce.*
3. Nella finestra di dialogo *Sicurezza di Windows*, seleziona *Aggiornamenti della protezione* > *Verifica disponibilità aggiornamenti*.

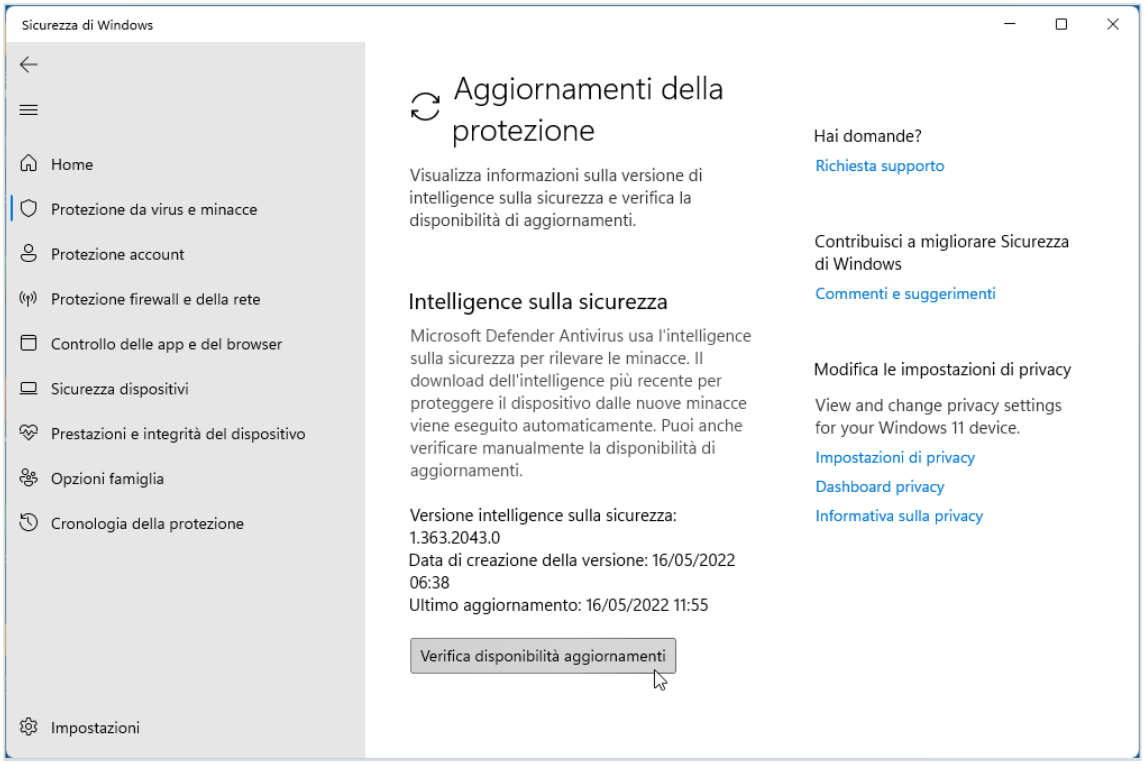



*Figura 2.5 — Verificare la disponibilità di aggiornamenti per Windows Defender*

**Attenzione.** Nessun antivirus può garantire la completa protezione dalle minacce informatiche. Il principale strumento per tenere al sicuro i propri dati personali è il buon senso. Di fatto, la colpa dell'elevata diffusione dei malware è da attribuire soprattutto a chi utilizza i computer: troppo spesso non ci curiamo delle più basilari misure di sicurezza, anche se immediatamente disponibili.

### 2.2.6. Avviare Windows Update

Una delle ragioni per cui sono molto spesso disponibili nuovi aggiornamenti per il sistema operativo *Windows* è l'incremento continuo della criminalità informatica. Gli sviluppatori di *Windows* infatti sono continuamente impegnati a trovare soluzioni sempre più efficaci, che possano rendere il sistema operativo meno attaccabile e suscettibile alle continue minacce informatiche che provengono da Internet.

Gli hacker in generale, o comunque tutti coloro che si impegnano per diffondere virus, worm, trojan, o altri malware, si accaniscono soprattutto con i dispositivi sui quali è installato il sistema operativo *Windows*. La ragione è molto semplice: oltre il 90 per centro dei computer che accedono costantemente a Internet utilizza questo sistema operativo.

Gli altri sistemi operativi sono altrettanto vulnerabili, ma meno diffusi. Per questo motivo, chi crea e diffonde malware preferisce tenerli da parte.

La necessità di dover rispondere a queste minacce ha spinto la *Microsoft* a creare un sistema basato sul web, con cui gli utenti di *Windows* possono controllare costantemente la disponibilità di nuovi aggiornamenti del sistema operativo, in modo da poterle scaricare e installare. Questo sistema prende il nome di *Windows Update*.

**Nota**. Gli aggiornamenti di solito contengono modifiche del codice del sistema operativo, che servono per renderlo più sicuro dagli attacchi informatici. Alcuni aggiornamenti invece vengono rilasciati per correggere alcuni difetti (non esiste il sistema perfetto, neanche nell'informatica!), o per migliorare le prestazioni hardware dei dispositivi su cui è installato il sistema operativo.

Per avviare *Windows Update*, segui questi passaggi:

1. Nella barra delle applicazioni di *Windows 11*, seleziona il pulsante *Start*  , quindi fai clic su *Impostazioni*  .
2. Nel menu a sinistra della finestra di dialogo *Impostazioni*, seleziona l'opzione *Windows Update*.
3. Seleziona il pulsante *Verifica la disponibilità di aggiornamenti*.

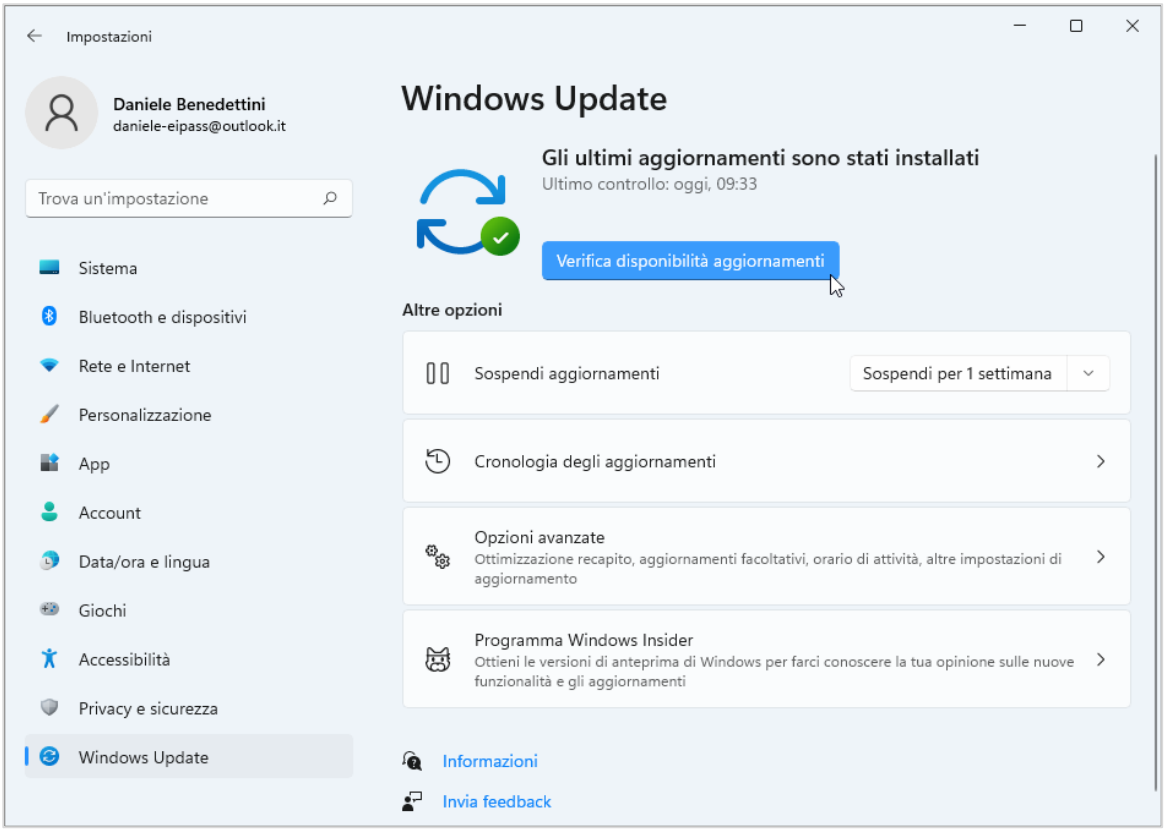



*Figura 2.6 — Avviare Windows Update*

# 3. Le reti informatiche e la loro sicurezza

## 3.1. I diversi tipi di reti informatiche

In informatica, si definisce *rete* (in inglese, *Network*) un gruppo di dispositivi (computer, smartphone, tablet, ecc.) collegati tra loro in modo che possano condividere file, documenti elettronici, e risorse, come stampanti, lettori multimediali, modem e memorie di massa.

È questo ciò che accade in molti uffici o aziende: tramite il suo computer, ogni operatore accede alla stessa banca dati cui accedono i computer degli altri operatori. Ogni operatore, dal proprio computer, invia la stampa a una sola stampante, condivisa con tutti gli altri operatori.

**Nota**. Una rete informatica può essere costituita da un numero indefinito di computer, da due all'infinito.

**Attenzione**. Più dispositivi possono essere in rete tra di loro, anche senza aver accesso a Internet. Le reti informatiche infatti non devono rimandarci necessariamente a Internet. Si possono costruire reti informatiche senza utilizzare Internet.

### 3.1.1. Le reti LAN e WLAN

È possibile classificare le reti informatiche a seconda della loro dimensione. Le reti LAN (*Local Area Network*) permettono a dispositivi relativamente vicini di comunicare tra di loro. Vengono infatti utilizzate per far sì che i dispositivi nello stesso spazio, come una abitazione, scuola, biblioteca o azienda, possano scambiarsi dati e informazioni, oltre a condividere stampanti, router, fotocopiatrici, ecc.

Le reti LAN utilizzano cavi di rete Ethernet per connettere i vari dispositivi. Proprio per questo motivo, vengono definite *cablate*.

Oltre a questo particolare tipo di cavi, per connettere i dispositivi alla stessa rete è necessario utilizzare un altro componente elettronico, chiamato NIC (*Network Interface*

*Card*, in italiano si traduce semplicemente con "Scheda di rete"). La scheda di rete è di solito integrata nelle schede madri dei laptop o dei computer desktop.

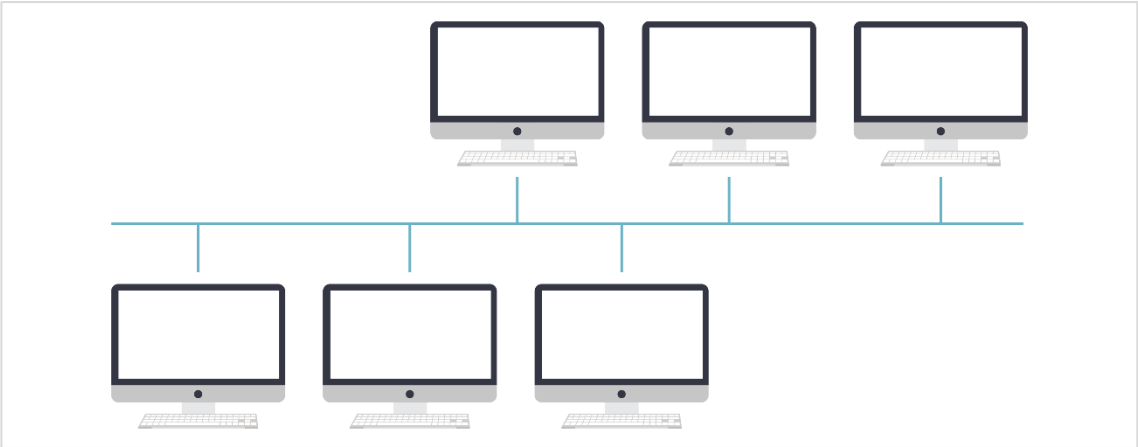


*Figura 3.1 — Lo schema di una rete LAN*

Negli ultimi anni si è imposta una nuova tecnologia di trasmissione dei dati che ha permesso di sostituire i cavi Ethernet con onde radio per creare reti informatiche. Si tratta delle così dette reti WLAN (*Wireless Local Area Network*).

La tecnologia che permette ai dispositivi collegati alla rete di trasmettere e ricevere segnali radio si chiama *Wireless*, e avviene in base allo standard *Wi-Fi*, il cui nome nasce dalla combinazione delle parole inglesi *Wireless-Fidelity*

Lo standard Wi-Fi definisce il modo in cui i segnali radio vengono inviati e ricevuti, ed è stato accettato a livello internazionale a partire dagli anni 2000. Prima di questa data, lo standard Wi-Fi manteneva la sua definizione ufficiale, ossia 802.11.

Messo a punto alla fine degli anni 90 del secolo scorso, lo standard 802.11 è stato oggetto di numerosi aggiornamenti, fino a quando si è deciso di dargli un nome più semplice da ricordare, ossia Wi-Fi.

I dispositivi più recenti, in particolare i notebook, i tablet e gli smartphone di tutti i tipi, dispongono dei componenti elettronici per collegarsi tramite il Wi-Fi a una rete WLAN, e questo li predispone a collegarsi a una rete informatica.

Le reti WLAN offrono maggiore sicurezza rispetto alle reti cablate. Impostando una password è infatti possibile proteggere la rete da eventuali tentativi di connessione non

autorizzati. Senza conoscere la password, non è possibile collegare alcun dispositivo alla rete.

Le reti WLAN sono quelle che comunemente utilizziamo nelle nostre abitazioni o negli uffici per far sì che più dispositivi possano accedere a Internet tramite lo stesso apparecchio, chiamato *router*.

Il *router*, a sua volta, utilizza un altro apparecchio elettronico, chiamato *modem*, per gestire il collegamento a Internet dei singoli dispositivi.

I dispositivi all'interno dalla rete WLAN posso pertanto utilizzare lo stesso punto di accesso (*router/modem*) per connettersi a Internet.

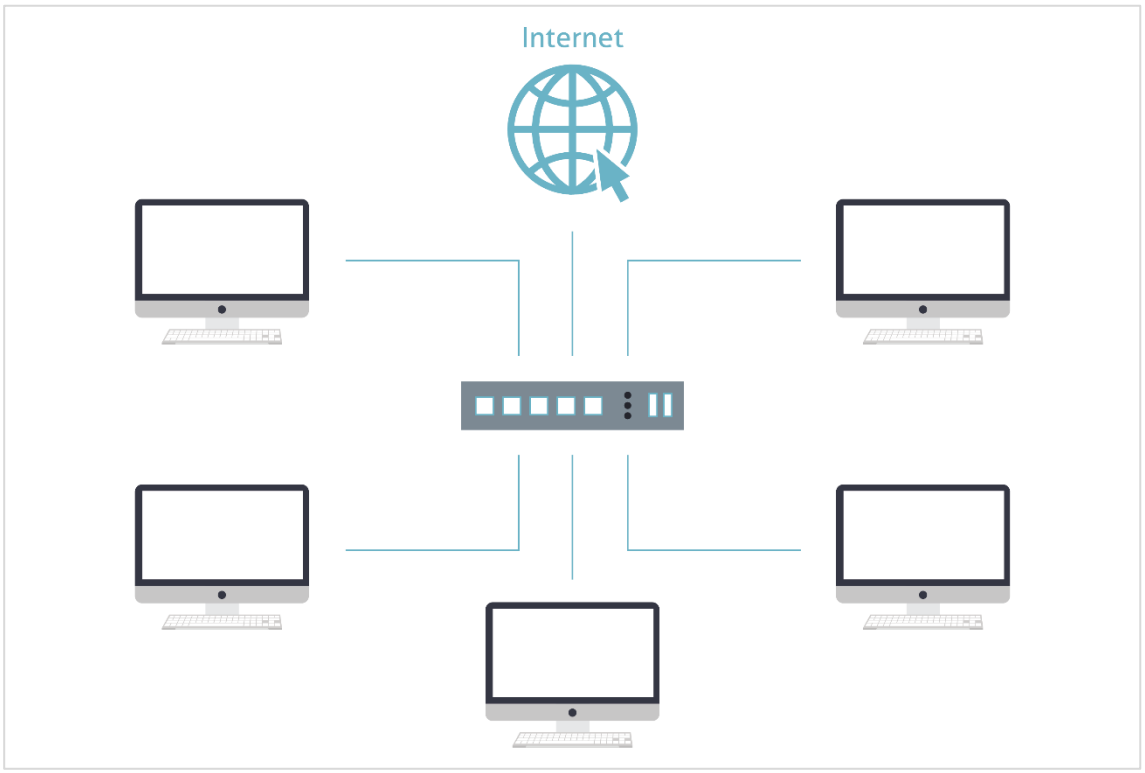



*Figura 3.2 — Lo schema di una rete WLAN*

**Nota**. La soluzione più comune al giorno d'oggi è quella di utilizzare un particolare apparecchio, il *modem/router*, per consentire a più dispositivi di collegarsi a Internet dallo stesso punto di accesso. Si tratta pertanto di un unico apparecchio che funge sia da *modem* che da *router*. La maggior parte dei *modem/router* in commercio sono muniti sia di porte Ethernet sia di apparecchi radio per connettere a Internet più dispositivi tramite il Wi-Fi.

### 3.1.2. Le reti MAN, WAN e VPN

Ci sono reti capaci di inglobare tutte le reti LAN di una grande città. Queste reti LAN si chiamano reti MAN (*Metropolitan Area Network*).

Con il passare del tempo, sono state create reti capaci di inglobare MAN sempre più grandi. Queste reti così estese si chiamano WAN (*Wide Area Network*). Internet ad esempio è una rete WAN: è infatti l'esempio più evidente del concetto di *rete di reti*.

Le reti VPN (*Virtual Private Network*, ossia "rete privata virtuale") sfruttano Internet per creare reti private. Sono pertanto un sistema sicuro per mettere in comunicazione computer e dispositivi che si trovano lontano l'uno dall'altro.

Internet infatti è una rete pubblica, che espone chiunque la utilizzi al rischio di possibili perdite dei propri dati personali, o più in generale, al pericolo di venire "spiati" durante la propria attività in rete.

Le reti VPN riducono questo rischio, visto che riescono a rendere private, e quindi più sicure, comunicazioni che avvengono tramite la più grande rete pubblica, ossia Internet.

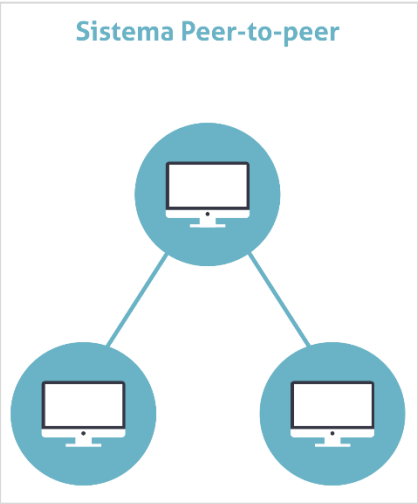
Le reti private sono più sicure semplicemente perché l'accesso è consentito soltanto alle persone autorizzate.

Le aziende utilizzano molto spesso questo tipo di reti per mettere in contatto diverse sedi delle loro attività. Le reti VPN infatti permettono alle aziende di utilizzare Internet per creare reti private con cui trasferire dati e informazioni in modo sicuro.

### 3.1.3. Le reti P2P e client/server

Le reti informatiche si distinguono inoltre in base al modo in cui vengono strutturate e utilizzate.

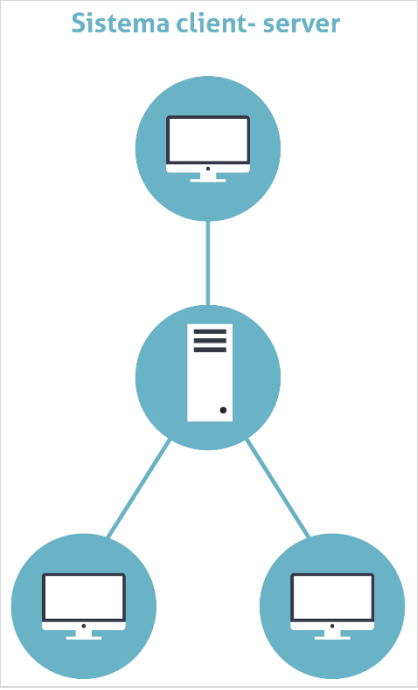
Ci sono reti in cui i singoli dispositivi collegati possono scambiarsi dati e condividere risorse in modo *paritario*, senza dover osservare alcuna gerarchia. Ciò significa che ciascun utente della rete può utilizzare il suo dispositivo per accedere ai contenuti presenti in tutti gli altri dispositivi della rete (che in questa particolare tipo di rete si chiamano "nodi").




Può ad esempio aprire un file o documento che si trova nel disco fisso di un altro computer della rete e visualizzarlo sullo schermo del suo dispositivo. Le reti di questo tipo, in cui i dispositivi collegati tra di loro sono tutti allo stesso livello, vengono definite *peer-to-peer* (dette anche *P2P*). La tecnologia P2P può comportare rischi per la sicurezza degli utenti della rete, ed elementi di illegalità relativi alla violazione dei diritti di copyright dei dati scambiati.

*Figura 3.3 — Lo schema di una rete P2P*

Molto spesso pertanto si preferisce creare una rete informatica in cui i dispositivi osservino una precisa *gerarchia* per comunicare tra di loro. In questo modo, è possibile ridurre il rischio che gli utenti della rete possano modificare o cancellare i file a loro piacimento, visto che nelle reti P2P ciascun utente può accedere a qualsiasi dispositivo della rete. Nelle reti P2P inoltre è impossibile stabilire l'affidabilità del nodo da cui stiamo scaricando i dati.




In pratica, non sappiamo se il computer dell'utente da cui stiamo acquisendo un file sia infettato con un malware o se l'utente stesso non usi questo sistema per riempirci di software infetti con i quali accedere successivamente al nostro computer.

Le reti organizzate in base a una precisa gerarchia vengono definite *client/server*. In queste reti, c'è un computer che governa tutti gli altri: i computer collegati alla rete (*client*) per interagire tra di loro devono ricevere l'autorizzazione dal computer dominante (*server*). Il server pertanto gestisce tutto il traffico dati che scorre tra i client della rete.

*Figura 3.4 — Lo schema di una rete client/server*

## 3.2. La sicurezza delle reti informatiche

Tutte le reti informatiche che abbiamo visto fin qui sono vulnerabili. Possono cioè subire attacchi da parte di malintenzionati, il cui fine è manometterle o acquisire i dati che i dispositivi della rete si trasmettono l'uno con l'altro.

### 3.2.1. Vulnerabilità delle reti informatiche

Gli attacchi alle reti informatiche possono provenire dagli utenti che non hanno le autorizzazioni per accedere a tutti i dati scambiati dai computer e dispositivi collegati. In questo caso, dalle reti informatiche potrebbero trafugare informazioni private, o più semplicemente, gli utenti della rete senza autorizzazione potrebbero visualizzare le informazioni loro precluse. Gli attacchi di questo tipo sono dunque interni alla rete stessa.

Se le reti vengono impiegate per consentire a più dispositivi di accedere a Internet (come ad esempio le reti WLAN), la prima minaccia alla loro sicurezza proviene dai malware che normalmente vengono diffusi in Rete, e che possono trovarsi — come abbiamo già visto — negli allegati alle email che riceviamo, nelle pagine web dei siti che visitiamo, o nelle applicazioni che scarichiamo gratuitamente da Internet. Gli attacchi di questo tipo sono dunque esterni alla rete.

Un'ultima causa di vulnerabilità delle reti informatiche è rappresentata dai così detti *stakeholders*, ossia da tutti i soggetti (aziende, persone, fornitori, clienti, ecc.) che a vario titolo sono coinvolti attivamente in un preciso progetto aziendale, e che pertanto hanno le autorizzazioni per accedere alla rete informatica dell'azienda con cui collaborano. Anche in questo caso è pertanto possibile che i soggetti esterni alla rete informatica possano accedere a dati e informazioni, che invece dovrebbero essere accessibili soltanto ai soggetti interni all'azienda.

### 3.2.2. Il ruolo dell'amministratore di rete

Normalmente ogni rete informatica è gestita da un amministratore (l'IT Manager).

Il primo compito dell'amministratore di rete è assegnare gli accessi ai singoli utenti. Ciascuno di loro deve poter disporre di un proprio account con cui accedere alla rete.

L'amministratore di rete inoltre organizza le autorizzazioni per ogni account. Ciò significa che può assegnare i così detti *privilegi*, ossia stabilire quali operazioni ciascun utente può eseguire, e quali invece sono a lui proibite.

Per migliorare la sicurezza della rete informatica, l'amministratore di rete gestisce il sistema con cui verificare l'identità di ciascun utente. Per accedere al proprio account, ogni utente dovrà pertanto inserire la password che gli è stata assegnata, o verificare la propria identità tramite un sistema di controllo delle impronte digitali o dei dati biometrici.

L'amministratore di rete inoltre si occupa della sicurezza del sistema. In questo ambito, il suo ruolo è quello di verificare la disponibilità di nuove *patch*, e di installarle. Le *patch* sono importanti aggiornamenti con cui rendere un sistema sempre più sicuro ed efficiente.

Sono le stesse case produttrici dei software a rilasciare le *patch* per rimediare ai così detti *bug*, ossia ai difetti di programmazione e di funzionamento del software riscontrati sino a quel momento. Le *patch* in particolare vogliono rimediare ai problemi di vulnerabilità che inevitabilmente interessano tutti i sistemi informatici.

L'amministratore di rete ha un altro importante ruolo: monitora costantemente il traffico dei dati che attraversano la rete, al fine di renderla sempre funzionante, e nello stesso tempo, vigila che nessun malware stia mettendo a rischio la sicurezza della rete.

### 3.2.3. Utilizzare un firewall per proteggere i dispositivi connessi a una rete

Gli antivirus a volte non sono sufficienti per bloccare i malware. Le reti informatiche infatti sono esposte a possibili infiltrazioni di software infetto, nonostante i nodi (i dispositivi connessi alla rete) siano protetti con un antivirus.

Per proteggere ulteriormente i nostri dispositivi dai pericoli che potrebbero provenire dalle reti informatiche, possiamo ricorre ai *firewall*. I firewall infatti sono specifici sistemi di sicurezza — hardware o software — che controllano il traffico dati sia in ingresso che in uscita dai dispositivi connessi a una rete locale o a Internet.

Funzionano in modo simile a un ufficio doganale: controllano sia i dati che attraverso la rete raggiungono i dispositivi dall'esterno, sia i dati che dai dispositivi si spostano verso l'esterno attraverso la rete.

**Attenzione**. I firewall non sono capaci di analizzare i dati in ingresso e in uscita alla ricerca di malware. I firewall definiscono le regole in base alle quali i dati possono entrare e uscire da un dispositivo quando è connesso a una rete, e pertanto consentono soltanto il traffico dati effettivamente autorizzato. Non svolgono dunque la stessa funzione degli antivirus, né funzionano in modo simile.

**Nota**. La parola *firewall* può essere tradotta in italiano con l'espressione "tagliafuoco", una speciale parete che negli edifici viene costruita per impedire agli incendi di propagarsi da una stanza all'altra. I firewall informatici svolgono una funzione simile: controllano il traffico dati in entrata e in uscita per bloccare le connessioni potenzialmente pericolose per i dispositivi collegati a una rete, e per i loro sistemi.

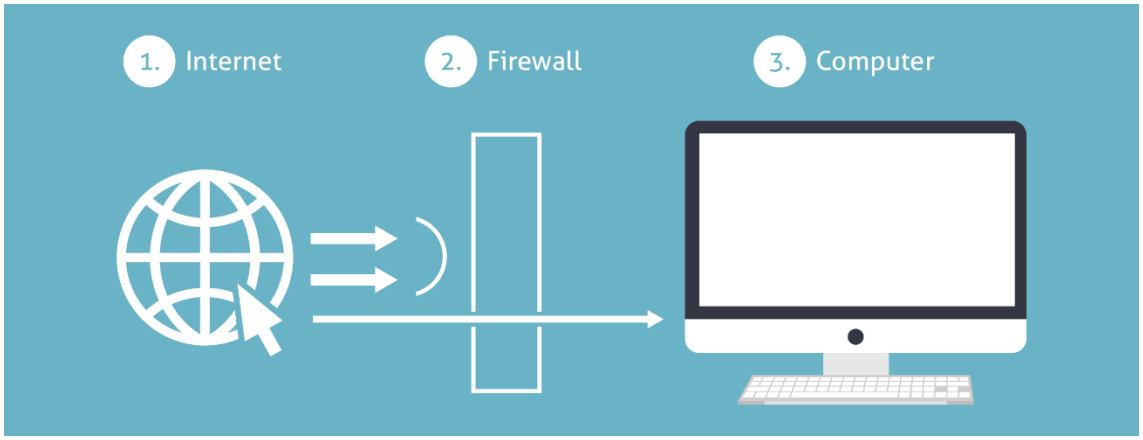



*Figura 3.5 — Funzionamento del firewall*

Il sistema operativo *Windows 11* ha già un firewall con cui proteggere i computer da possibili infezioni che possono provenire dall'esterno.

In *Windows 11*, per configurare il firewall, procedi come segue:

1. Nella barra delle applicazioni di *Windows 11*, seleziona il pulsante *Start*, quindi fai clic su *Impostazioni*.
2. Nel menu a sinistra della finestra *Impostazioni*, seleziona *Privacy e sicurezza* > *Sicurezza di Windows* > *Firewall e protezione rete*.
3. La finestra di dialogo *Sicurezza di Windows* è impostata per mostrare la sezione da cui configurare il firewall di *Windows 11* (vedi la Figura 3.6).
4. Nelle sezioni *Rete di dominio*, *Rete privata* e *Rete pubblica*, verifica che la barra di scorrimento sia posizionata su *Attivato*. In questo modo, avrai la certezza che il tuo

dispositivo sia protetto dal firewall di *Windows* ogni volta che si collegherà a una rete.

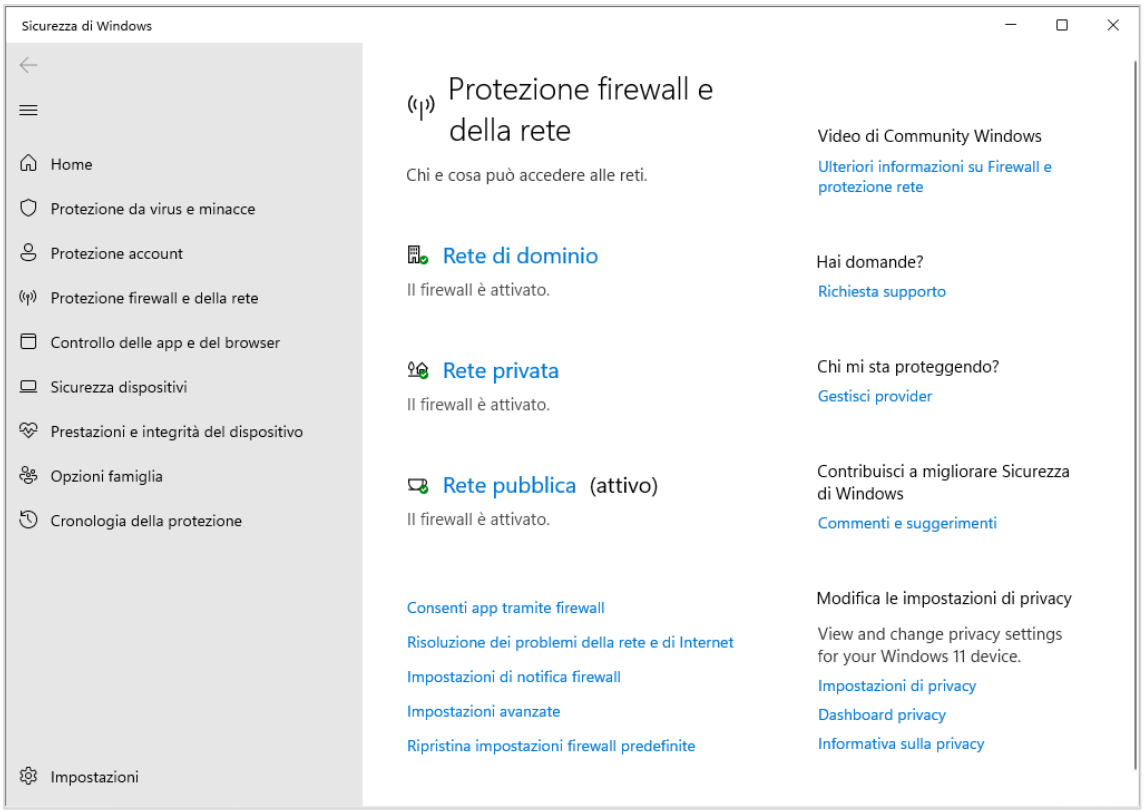



*Figura 3.6 — La finestra di dialogo di Windows 11 da cui configurare il firewall*

I firewall ci segnalano quando un'applicazione installata sul nostro dispositivo cerca per la prima volta di connettersi a una rete (come Internet), e inoltre ci segnalano tutti i tentativi esterni di intrusione. In questi casi, possiamo decidere cosa fare: consentire lo scambio dei dati, oppure impedirlo.

## 3.3. La sicurezza nelle reti wireless

L'utilizzo dei cavi per collegare i dispositivi e creare una rete locale è ormai in disuso. Da diversi anni infatti si utilizza la tecnologia wireless per connettere più dispositivi alla stessa rete. Il wireless utilizza segnali radio anziché cavi per trasferire dati. È dunque il sistema più comodo per collegare il proprio dispositivo a una rete. Come visto in precedenza, le reti di questo tipo si definiscono WLAN (*Wireless Local Area Network*), o più semplicemente *Reti wireless*.

### 3.3.1. I diversi tipi di attacchi alle reti wireless

Il primo tipo di attacco a cui sono soggette le reti wireless che non rispettano i sistemi di sicurezza che abbiamo enunciato nei paragrafi precedenti si chiama *eavesdropping*.

L'etimologia della parola *eavesdropping* (in italiano significa "origliare") è davvero evocativa, e da subito l'idea di un malcostume vecchio quanto il mondo. L'*eavesdropping* indica l'atto del malintenzionato di ascoltare conversazioni altrui e di registrare tutte le informazioni che riesce a carpire, come per esempio username e password.

Si parla, in definitiva, di una tecnica di intercettazione. In questo contesto, ascoltare vuol dire recupere dati e leggerli alla ricerca di tracce importanti. Per esempio, alcuni hacker creano volutamente reti wireless non protette, in modo che altre persone possano trovare conveniente collegarsi. In questo modo, gli hacker riescono a intercettare i dati di chi si collega alla rete.

Un altro tipo di attacco a cui sono soggette le reti wireless è il così detto *jamming* (in italiano si potrebbe tradurre con la parola "interferire"). In questo caso, gli hacker vogliono dirottare le comunicazioni radio che avvengono tra il punto di accesso alla rete wireless e i dispositivi ad essa connessi, per convogliarle su un altro punto di accesso, in modo da trafugare le informazioni personali di chi si connette alla rete.

Il *network hijacking* (in italiano si potrebbe tradurre con l'espressione "dirottamento di rete") è quella particolare tecnica con cui gli hacker riescono a reindirizzare le persone connesse a una rete wireless verso siti carichi di malware.

L'attacco hacker che prende il nome di *Man in the middle* (letteralmente "uomo nel mezzo") è il modo più semplice di carpire informazioni personali sugli utenti di una rete wireless.

In questo caso, gli hacker si inseriscono in una conversazione privata per leggere i messaggi inviati, modificarli o inserirne altri. In questo caso, lo scopo degli hacker è violare la privacy dei partecipanti alla conversazione, e di carpire le loro informazioni personali. In altri casi, gli hacker si interpongono in una comunicazione, fingendo di essere una delle due parti coinvolte o entrambe. Lo si può fare, ad esempio, accedendo al microfono dello smartphone o del tablet e convincendo i malcapitati a comunicare i propri dati sensibili a quello che credono essere il proprio amico.

### 3.3.2. L'importanza delle password per accedere alle reti wireless

I computer e i dispositivi mobili più recenti sono già dotati dei componenti elettronici necessari per trasmette e ricevere segnali radio in base allo standard di comunicazione Wi-Fi. Ciò significa che possono sfruttare il wireless per connettersi a una rete locale senza ulteriori attrezzature.

Per garantire la sicurezza delle reti wireless, è possibile configurare una password con cui accedervi. In pratica, se una rete wireless non è protetta con una password, chiunque nelle vicinanze potrebbe collegarsi senza alcuna difficoltà. Per un esperto informatico tuttavia non è difficilissimo violare la password. Ci sono infatti diversi programmi che consentono di aggirarla. Nonostante ciò, la configurazione di una password per accedere alla propria rete wireless scoraggerà di certo molti estranei a tentare di collegarsi alla rete.

Di solito, la maggior parte dei router/modem che troviamo in commercio hanno già una password che dobbiamo inserire nel nostro computer o dispositivo per far sì che possa connettersi alla rete wireless. Sul retro di molti modem/router troviamo una tabella simile a quella che segue, con le informazioni per collegare un computer o dispositivi mobili alla rete WLAN e LAN.

| | |
|---|---|
| Rete wireless | Home&Life SuperWiFi-2F29 |
| Password wireless | CV3PHPPARD34XYPO |
| Indirizzi IP modem | https://192.168.1.1 |
| Username | admin |
| Password | Vyfx99Ytfr |

*Tabella 3-1 — Le informazioni che potremmo trovare sul retro di un router/modem per accedere alla rete WLAN e LAN*

Le prime due righe della tabella in questo caso ci dicono il nome predefinito della rete WLAN (wireless), e la password con cui accedervi. Le tre righe successive invece ci dicono l'indirizzo IP del modem (questo indirizzo è decisivo per identificare in modo univoco il modem all'interno della rete), la username e la password con cui accedere alla rete LAN. Molti modem/router infatti creano sia reti WLAN che LAN per consentire a più dispositivi

di accedere a Internet. Nel caso in cui volessimo sfruttare la rete LAN per collegare il nostro dispositivo a Internet, dobbiamo ricordarci di utilizzare un cavo Ethernet che colleghi il dispositivo al modem/router.

**Nota**. Inserisci l'indirizzo IP del modem nel tuo browser preferito. Nella pagina web che compare nella finestra del browser, inserisci la username e la password. Così facendo, accedi virtualmente al tuo router/modem, e puoi modificarne le configurazioni di rete.

### 3.3.3. I protocolli di sicurezza per le reti wireless

Al giorno d'oggi, le reti wireless sono ovunque. Le troviamo nei bar, nei ristoranti, nelle scuole, negli uffici, nelle Università, e così via. Quando colleghiamo il nostro dispositivo a una di queste reti, dobbiamo chiederci quanto sia sicura. Un buon inizio è controllare le impostazioni di sicurezza della rete per capirne il livello di protezione.

Esistono vari protocolli di sicurezza per le reti wireless. Questi protocolli sono stati creati dalla *WiFi Alliance*, un'organizzazione formata da circa trecento industrie leader nel settore, nata nel 1999 con lo scopo di promuovere l'adozione di un unico standard senza fili per la "banda larga" (una tecnica che offre un ventaglio — una banda, appunto — di velocità di connessione molto ampio). La stessa organizzazione è inoltre proprietaria del trademark Wi-Fi.

Il protocollo WEP (*Wired Equivalent Privacy*, in italiano significa "Sicurezza della privacy equivalente") viene dichiarato standard per la sicurezza Wi-Fi nel settembre del 1999, quando si sostiene che riesca ad assicurare lo stesso livello di sicurezza delle reti cablate.

In realtà, oltre a essere difficile da configurare, possiede falle di sicurezza ben conosciute che lo rendono facile da sorpassare. La *WiFi Alliance* pertanto decide di abbandonarlo definitivamente nel 2004.

Il protocollo WPA (*Wi-Fi Protected Access*, che in italiano significa grossomodo "Accesso protetto alla rete Wi-Fi") è il risultato del miglioramento del protocollo WEP. È stato adottato nel 2003, soprattutto perché compatibile con i dispositivi che utilizzavano il protocollo WEP.

Il protocollo WPA tuttavia non ha migliorato molto la sicurezza delle reti wireless, ma ha reso la loro configurazione molto più semplice.

Dipendendo molto dalla vecchia tecnologia WEP, il protocollo WPA ha riscontrato molte vulnerabilità, ed è pertanto risultato molto suscettibile alle intrusioni dannose.

Nel 2004, è stata pertanto rilasciata la seconda versione del protocollo WPA. Il protocollo WPA2 rappresenta un passo in avanti in termini di sicurezza delle reti wireless. La sua differenza principale rispetto al protocollo WPA è che utilizza il sistema di cifratura AES (*Advanced Encryption Standard*). Anche il governo americano utilizza lo stesso sistema per criptare informazioni di importanza cruciale. Questo ci fa capire quanto il protocollo WPA2 sia più sicuro rispetto ai protocolli precedenti.

In alcune situazioni, anche il protocollo WPA2 si è rivelato poco sicuro: se un hacker riesce a entrare nella rete wireless, nonostante utilizzi un protocollo di sicurezza, a quel punto può attaccare tutti i dispositivi connessi.

Il protocollo WPA2 riesce pertanto a garantire una buona sicurezza delle reti wireless quando gli attacchi provengono dall'esterno, ma non garantisce la stessa cosa quando provengono dall'interno della rete.

**Nota**. WPA2 è un protocollo di sicurezza più recente che è stato progettato per correggere alcune vulnerabilità di sicurezza presenti nell'originale WPA. Il Protocollo WPA, come il WPA2, ha due modalità: *personal* e *enterprise*. La modalità *personal* è adatta alle reti domestiche. Una volta impostata una password, tutti color che vogliono utilizzare quella determinata rete wireless devono inserirla al momento della connessione. La modalità *enterprise* è adatta alle reti aziendali. È più complicata da impostare, ma offre un controllo centralizzato e personalizzato sull'accesso alla rete wireless. Al momento della connessione, ogni utente inserisce la propria username, senza password. Il sistema di criptazione delle chiavi di accesso lavora in background, assegnandone automaticamente una a ogni utente per ogni sessione.

Man mano che vengono scoperte nuove vulnerabilità delle reti informatiche, i tecnici si impegnano per trovare soluzioni alternative con cui risolverle. È per questo che il mondo dell'informatica continua a progredire.

Nel 2018, *Wi-Fi Alliance* ha annunciato l'avvento del protocollo di sicurezza WPA3. Più sicuro ed efficiente del suo predecessore, il protocollo WPA3 non è ancora molto diffuso.

## 3.4. Gli hotspot

Gli *hotspot* sono punti di accesso a Internet, ai quali è possibile collegarsi tramite il Wi-Fi. In questo modo, è possibile utilizzare il proprio dispositivo per navigare in Internet, senza utilizzare la rete mobile.

### 3.4.1. Cos'è e come funziona un hotspot

I centri commerciali, le stazioni, gli aeroporti, i bar, le scuole e le Università sono luoghi da cui è possibile accedere a Internet gratuitamente, attraverso il proprio dispositivo. Ciò avviene perché questi luoghi sono un hotspot, ossia un punto di accesso a Internet.

Una volta entrarti in questi luoghi, è sufficiente attivare il Wi-Fi sul proprio dispositivo per visualizzare il nome della rete wireless a cui connettersi per accedere a Internet. In questo modo, possiamo evitare di utilizzare la nostra rete mobile, che in molti casi ha un costo in base ai dati che consumiamo durante la navigazione.

In molti casi, se attiviamo il Wi-Fi mentre siamo seduti in un tavolo di un ristorante o bar, ci viene segnalata la presenza della rete wireless del locale. Se proviamo a collegarci, può accadere che ci venga richiesta una password.

Come abbiamo già visto, le password vengono configurate con il preciso scopo di rendere le reti wireless più sicure, visto che soltanto chi conosce la password può accedervi.

Tuttavia, la password è anche una forma di tutela per chi mette a disposizione l'hotspot, perché in questo modo scarica la responsabilità di ciò che viene fatto online su chi sta effettivamente usando la connessione. L'autenticazione consente infatti di risalire agli orari di navigazione e ai contenuti attivati da ogni cliente (è una tutela per il gestore, ma anche per gli altri clienti).

In altri casi, le reti wireless sono disponibili senza eseguire alcuna procedura di autenticazione. È il caso ad esempio dei luoghi pubblici come ad esempio degli aeroporti, in cui basta avviare il Wi-Fi per conoscere la rete wireless a cui possiamo connetterci.

Gli hotspot possono trovarsi sia in luoghi pubblici che privati, come nelle nostre abitazioni. I router/modem che comunemente installiamo nelle nostre case infatti costituiscono un hotspot, visto che permettono a tutti i dispositivi ad essi collegati di accedere a Internet.

### 3.4.2. Configurare un hotspot personale: il tethering

Da diverso tempo a questa parte, possiamo utilizzare il nostro smartphone o tablet per consentire ad altri dispositivi di accedere a Internet. In pratica, il nostro dispositivo mobile può fungere da hotspot. In questo caso, si parla di *tethering*.

Il *tethering* può esserci utile quando ad esempio ci troviamo in un luogo in cui è assente la connettività a Internet, oppure costa troppo. Possiamo in questi casi accedere a Internet sfruttando, ad esempio, la connessione di un nostro amico.

In un dispositivo mobile che utilizza il sistema operativo *Android*, per attivare il *tethering*, segui questi passaggi:

1. Apri l'app *impostazioni*
2. Seleziona *Connessioni* > *Router Wi-Fi e tethering* > *Router Wi-Fi*.
3. Fai tap su *Configura*.
4. Inserisci il nome che desideri assegnare alla rete wireless del tuo dispositivo mobile. Questo nome sarà quello che le altre persone visualizzeranno sui loro dispositivi quando vorranno collegarsi al tuo dispositivo mobile per accedere a Internet.
5. Scegli se proteggere o meno la rete wireless con una password. Le reti wireless non protette sono spesso rischiose. Pertanto è sempre meglio scegliere il protocollo di sicurezza con cui trasferire i dati, e configurare una password per accedervi.
6. Fai tap su *Salva*.
7. Adesso che hai configurato il tuo hotspot personale, non ti resta che abilitarlo. Nella scheda *Router Wi-Fi*, fai dunque tap sulla barra superiore.

Il tuo hotspot è adesso in funzione. Per collegare ad esso un dispositivo, come un computer, uno smartphone, un laptop o un tablet, occorre (1) aprire il menu con l'elenco

delle reti Wi-Fi a cui è possibile collegarsi, (2) selezionare il nome della rete che hai creato prima di attivare il tuo hotspot, (3) e inserire la password da te scelta.

Per disattivare il *tethering*, apri l'app *Impostazioni* sul tuo dispositivo mobile, e poi seleziona *Connessioni* > *Router Wi-Fi e tethering* > *Router Wi-Fi*. Fai tap sulla barra superiore per disattivare il servizio il tethering.

# 4. Misure per navigare sicuri in Internet

## 4.1. Il browser e la sicurezza online

Per rendere più sicura la navigazione in Internet, è possibile configurare il browser, affinché si riducano le possibilità di subire una perdita dei dati personali. I browser più recenti infatti danno la possibilità ai loro utenti di personalizzare i livelli di sicurezza per navigare in Internet, lasciandoli liberi di bloccare o meno determinati elementi che girano online.

### 4.1.1. Gestire le password

I browser hanno un'utile funzione per salvare le password. In pratica, quando creiamo un account su un sito web, il browser ci permette di salvare le credenziali che abbiamo scelto durante la registrazione. In questo modo, sarà per noi più semplice accedere ai nostri account le volte successive, visto che il browser inserisce automaticamente le password da noi memorizzate.

**Nota**. Nel browser *Google Chrome*, le password che decidiamo di salvare vengono memorizzate nel nostro account *Google*, in modo da poterle usare su qualsiasi dispositivo. Tramite la sincronizzazione infatti alcune informazioni, come ad esempio la cronologia delle pagine web da noi visitate, le password di accesso ai nostri account, gli indirizzi web che abbiamo aggiunto ai preferiti, sono disponibili su ogni dispositivo che utilizziamo per accedere al nostro account *Google*.

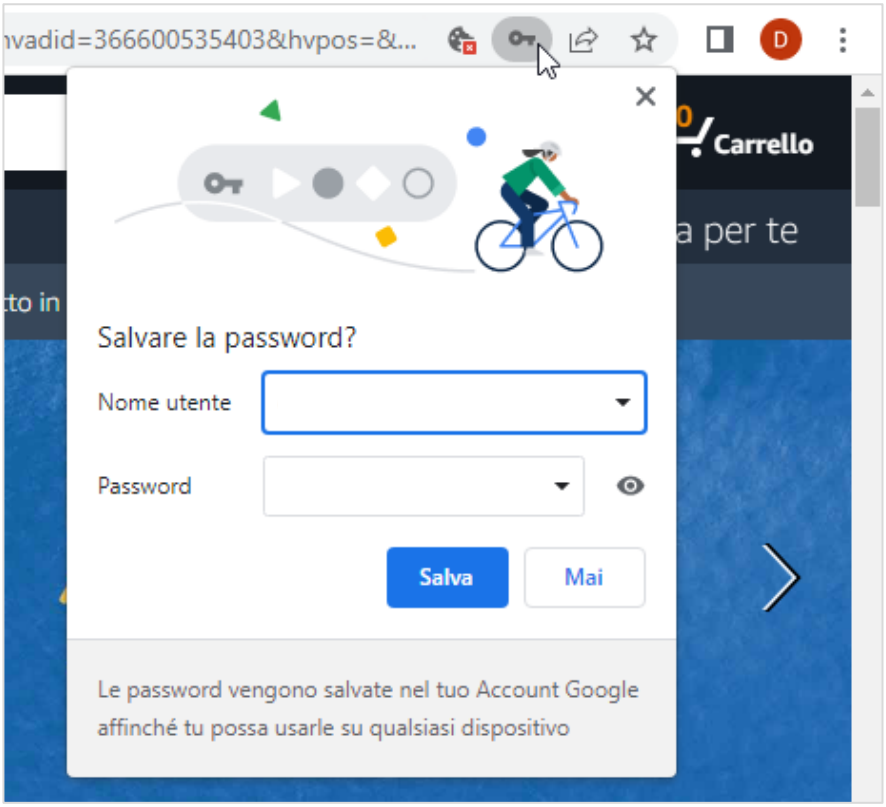



*Figura 4.1 — La finestra di Google Chrome da cui salvare le password*

Memorizzare le password è molto comodo. Ci sono però seri rischi per la nostra sicurezza: chi accede ai nostri dispositivi può accedere anche ai nostri account. Sarebbe pertanto meglio evitare di memorizzare le password, o perlomeno scegliere quali password memorizzare.

Nel browser *Google Chrome* per disattivare la funzione con cui memorizzare le password, segui questi passaggi:

1. Seleziona il pulsante *Personalizza e controlla Google Chrome*. L'icona di questo pulsante è costituita da tre puntini verticali, e si trova all'estremità destra della barra degli indirizzi.
2. Nel menu che si apre, seleziona l'opzione *Impostazioni*.
3. Nel menu a sinistra della scheda *Impostazioni*, seleziona l'opzione *Compilazione automatica*, quindi fai clic su *Password*.
4. Come impostazione predefinita, quando inserisci una nuova password, *Google Chrome* ti propone di salvarla. Per disattivare questa funzione, sposta verso sinistra

la barra in corrispondenza di *Chiedi di salvare le password*. Così facendo, ogni volta che vorrai accedere nei tuoi account, dovrai inserire sia la username che la password, perché *Google Chrome* non le avrà memorizzate.

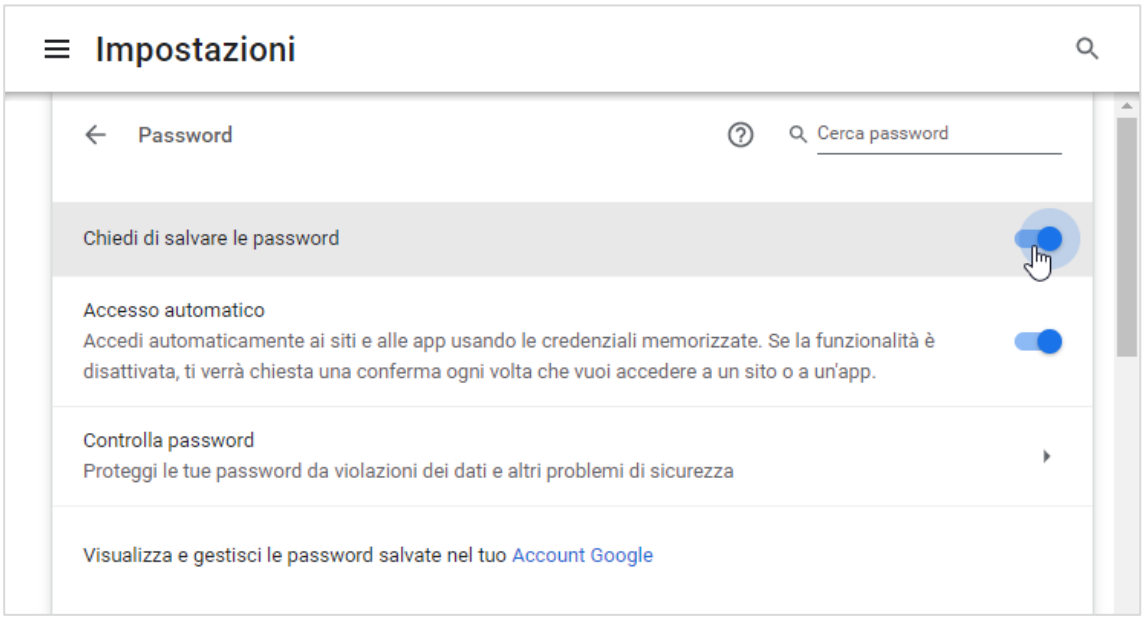



*Figura 4.2 — Disattivare la funzione di Google Chrome per memorizzare le password*

Se tuttavia hai memorizzato le tue password, puoi comunque cancellarle. Nella scheda *Impostazioni* di *Google Chrome*, visualizzi l'elenco dei siti web le cui password sono state memorizzate nel tuo account *Google*. In corrispondenza dell'indirizzo web del sito di cui desideri cancellare la password, fai clic sul pulsante con tre puntini verticali, e nel menu che si apre, seleziona l'opzione *Rimuovi*.

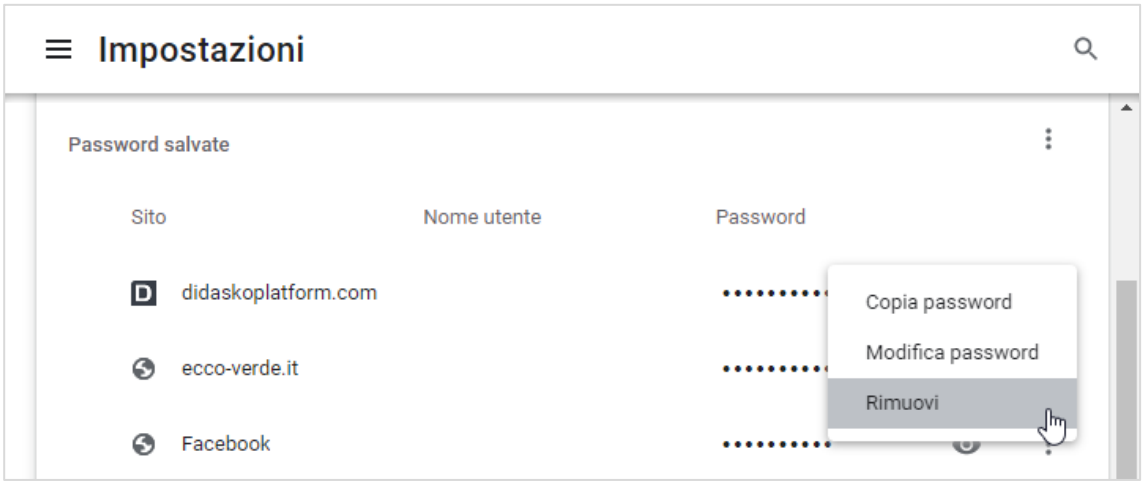



*Figura 4.3 — Rimuovere una password salvata nel proprio account Google*

Se hai deciso di memorizzare le password, puoi eseguire un controllo di sicurezza, in modo da valutare se sono state compromesse in seguito a una violazione dei dati, o se sono potenzialmente inefficaci e facili da indovinare.

Per controllare le password che hai salvato, nella scheda *Impostazioni* di *Google Chrome*, seleziona l'opzione *Controlla password* > *Controlla*.

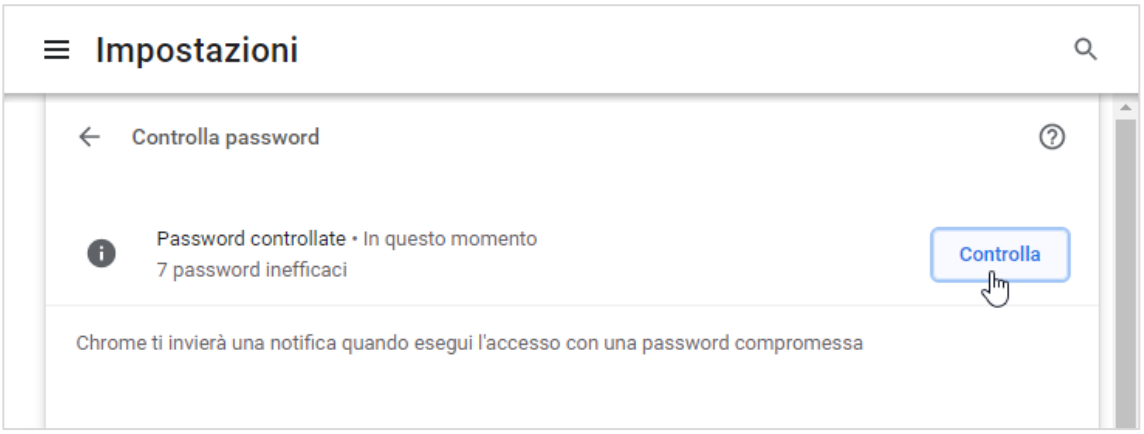



*Figura 4.4 — Eseguire il controllo di sicurezza delle password salvate*

Al termine del controllo, *Google Chrome* mostra una lista con gli indirizzi dei siti web le cui password sono inefficaci. Seleziona dunque il pulsante *Cambia password* in corrispondenza dell'indirizzo web del sito la cui password desideri modificare. *Google Chrome* ti collegherà automaticamente alla pagina del sito da cui puoi modificare la password.

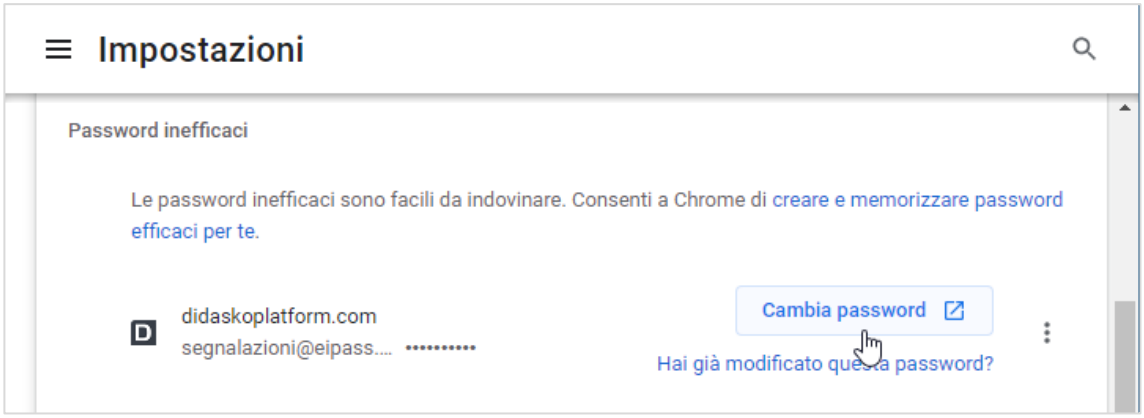



*Figura 4.5 — Cambiare una password inefficace*

### 4.1.2. Compilare automaticamente i moduli online

Nella maggior parte dei browser possiamo memorizzare le nostre informazioni personali, in modo da compilare automaticamente i moduli online.

I moduli online sono composti da diversi campi, nei quali possiamo inserire le nostre informazioni personali, come ad esempio numeri di telefono, indirizzi email e indirizzi di spedizione.

Servono a comunicare le nostre informazioni quando ci vengono richieste (ad esempio, prima di eseguire un acquisito online, o di accedere a un servizio).

Questa funzione è tanto comoda, quanto rischiosa per la nostra privacy, soprattutto se il nostro dispositivo è utilizzato da più persone.

Come per le password, sarebbe pertanto meglio disattivare la funzione per compilare automaticamente i moduli online, o quanto meno imparare a gestirla nel modo migliore per tutelare le nostre informazioni personali.

Nel browser *Google Chrome*, per memorizzare le tue informazioni personali, in modo da inserirle automaticamente nei moduli online che devi compilare, segui questi passaggi:

1. Seleziona il pulsante *Personalizza e controlla Google Chrome*. L'icona di questo pulsante è costituita da tre puntini verticali, e si trova all'estremità destra della barra degli indirizzi.
2. Nel menu che si apre, seleziona l'opzione *Impostazioni*.
3. Nel menu a sinistra della scheda *Impostazioni*, seleziona l'opzione *Compilazione automatica*, quindi fai clic su *Indirizzi e altro*.
4. Sposta verso destra la barra in corrispondenza dell'opzione *Salva e compila gli indirizzi*, quindi fai clic sul pulsante *Aggiungi*.
5. Nella finestra *Aggiungi indirizzo*, compila i campi come richiesto.
6. Fai clic sul pulsante *Salva*.

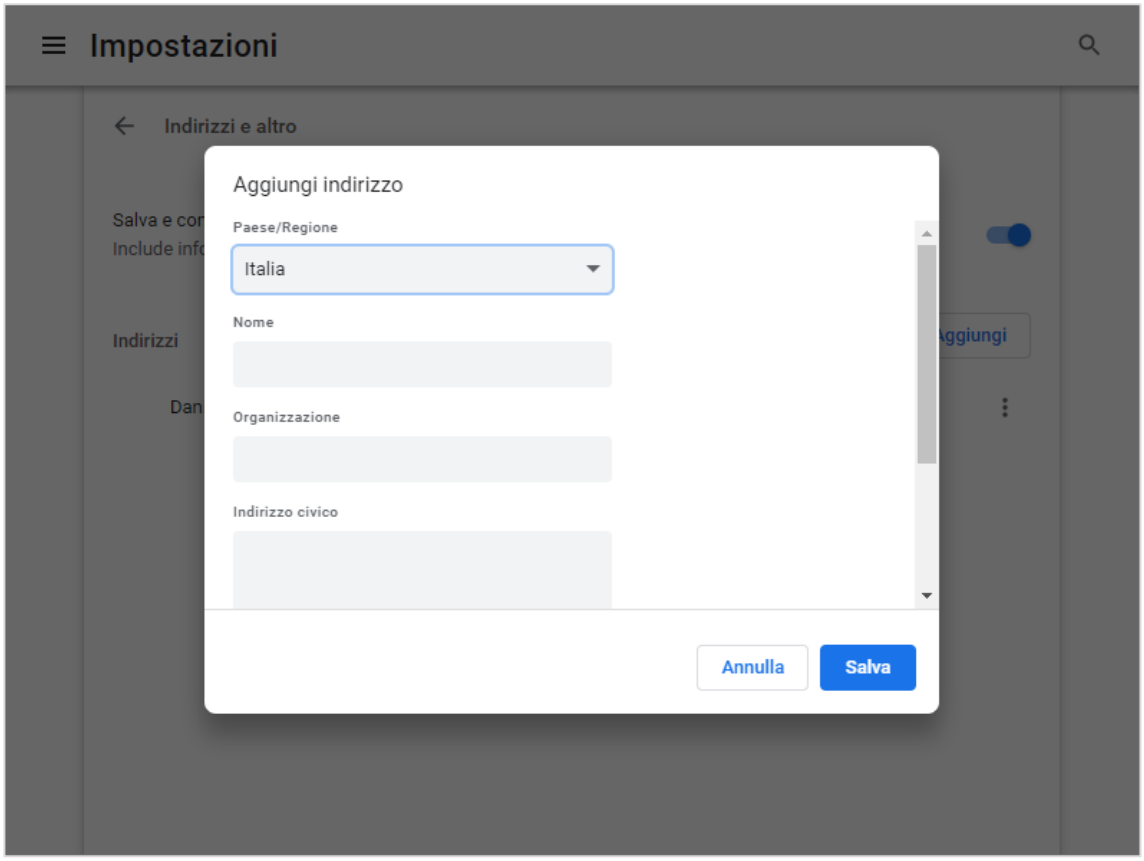



*Figura 4.6 — Memorizzare i propri dati personali in Google Chrome per compilare automaticamente i moduli online*

Le informazioni da te inserite compaiono nella sezione *Indirizzi*.

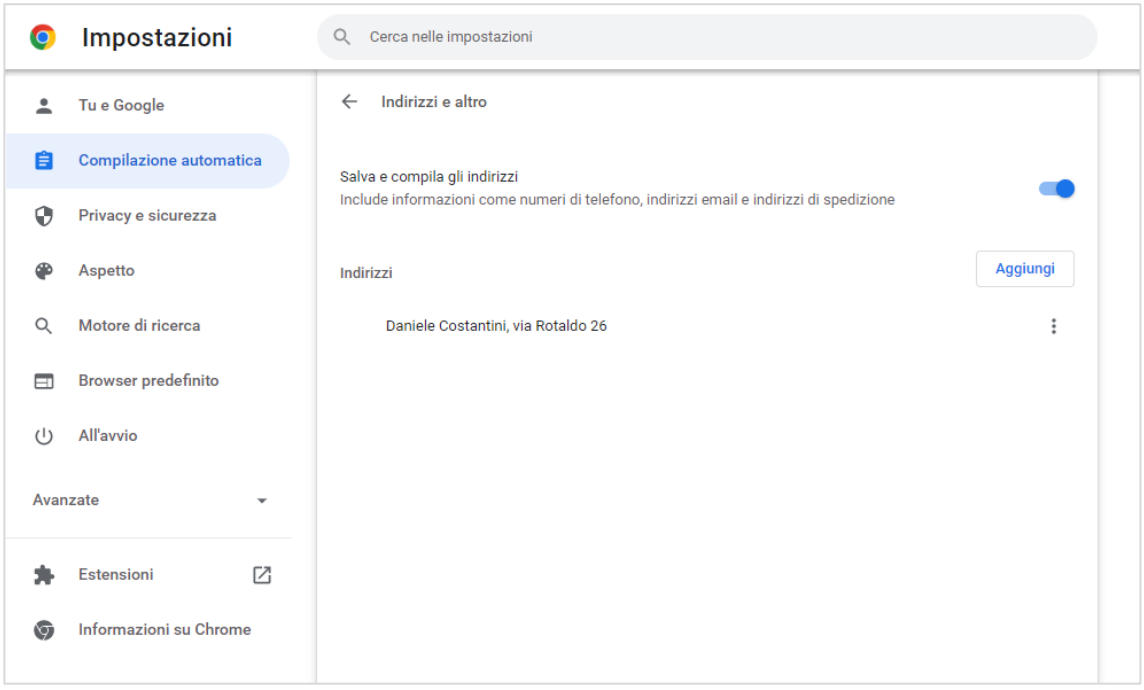



*Figura 4.7 — Aggiungere un indirizzo a Google Chrome per compilare moduli online*

La prossima volta che dovrai compilare un modulo online, fai clic sul primo campo, e seleziona l'informazione da inserire nel menu che si apre sotto il campo stesso.

**Nota**. Oltre ai dati personali, puoi memorizzare i dati della tua carta di credito. In *Google Chrome*, apri la scheda *Impostazioni*, e seleziona *Compilazione automatica > Metodi di pagamento*. Attiva dunque la funzione *Salva e compila i metodi di pagamento*, e poi fai clic su *Aggiungi*. Compila i campi come richiesto, e poi fai clic su *Salva*.

### 4.1.3. Cancellare la cronologia del browser

Mentre navighiamo in Internet, il nostro browser conserva una lista di tutte le pagine web che abbiamo visitato. Questa lista prende il nome di *cronologia*.

La cronologia è uno strumento utile quando desideriamo tornare a distanza di tempo su una pagina web che sappiamo avere notizie di nostro interesse, ma non ricordiamo il suo indirizzo (l'URL).

Indirettamente, però, può rappresentare una minaccia per la nostra privacy: chiunque abbia accesso al nostro computer, infatti, può conoscere le pagine da noi visitate di recente.

Potremmo pertanto decidere di cancellare la cronologia periodicamente (ogni settimana, ogni mese, e così via), oppure dopo ogni sessione di navigazione in Internet.

Ogni browser ha un comando per cancellare la cronologia. In *Google Chrome* per cancellare la tua cronologia, procedi come segue:

1. Seleziona il pulsante *Personalizza e controlla Google Chrome*. L'icona di questo pulsante è costituita da tre puntini verticali, e si trova all'estremità destra della barra degli indirizzi.
2. Posiziona il cursore sull'opzione *Cronologia*, e nel sotto-menu apertosi, fai clic di nuovo su *Cronologia*.
3. Nel menu a sinistra della scheda *Cronologia*, seleziona l'opzione *Cancella dati di navigazione*.
4. Nella finestra di dialogo che si apre, togli il segno di spunta dalle opzioni *Cookie e altri dati dei siti* e *Immagini e file memorizzati nella cache*.

5. Fai clic su *Cancella dati*.

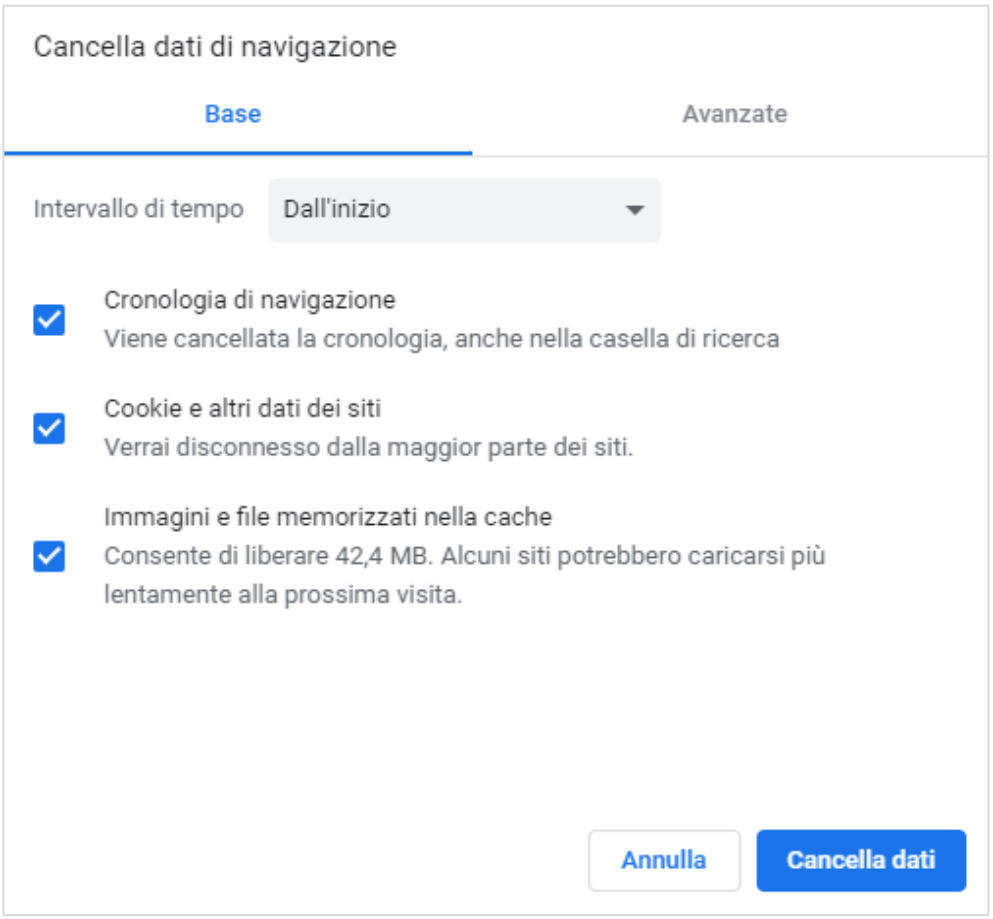



*Figura 4.8 — Cancellare i dati di navigazione dal browser Google Chrome*

**Suggerimento**. Apri il menu che si trova nell'area superiore della finestra di dialogo *Cancella dati di navigazione* (vedi la Figura 4.8), e scegli l'intervallo di tempo entro cui cancellare la cronologia. L'opzione *Dall'inizio* cancella tutti i dati di navigazione della cronologia.

## 4.2. Navigare in sicurezza

Un altro aspetto importante della sicurezza in Internet è quello relativo alla protezione degli utenti mentre navigano in Internet.

### 4.2.1. Capire quando un sito web è sicuro

Durante la navigazione in Internet, il browser ci comunica il livello di sicurezza del sito sul quale ci troviamo, e lo fa attraverso delle icone, che compaiono all'estrema sinistra della barra degli indirizzi.

ora non ¯ pi½cos³

Se, nella barra degli indirizzi del browser, compare un lucchetto chiuso prima dell'URL, significa che il sito in cui ci troviamo è sicuro (vedi la Figura 4.9).

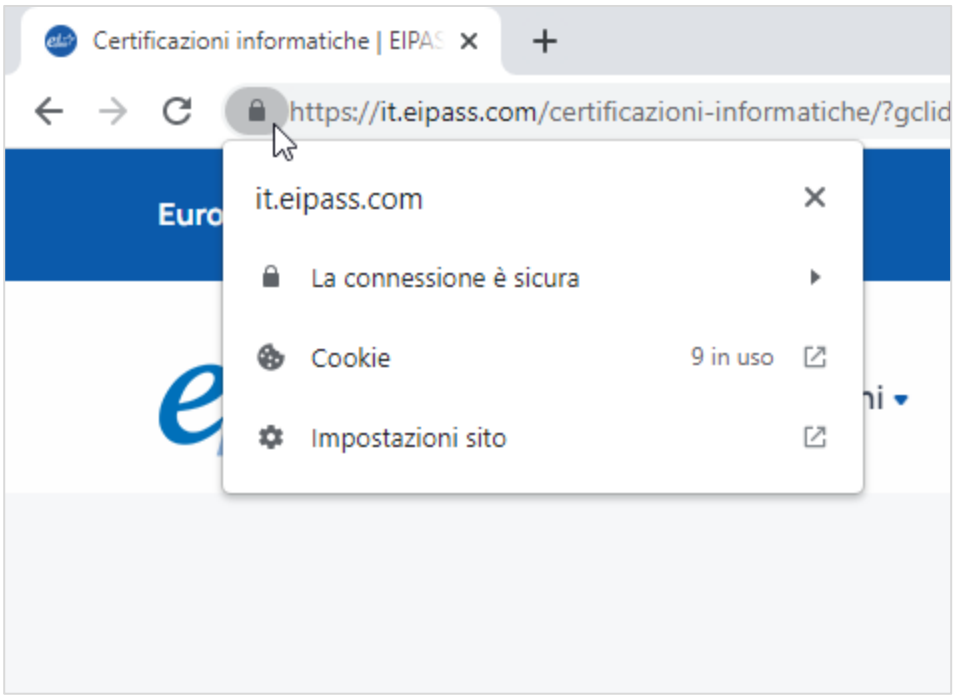



*Figura 4.9 — Il lucchetto indica quando un sito web è sicuro*

Se anziché il lucchetto, compare l'icona grigia con il punto esclamativo, significa che il sito in cui ci troviamo non è sicuro. Il sito in questo caso non utilizza una connessione privata. Qualcuno pertanto potrebbe riuscire a visualizzare e modificare le informazioni che scambiamo con il sito. Proprio per questo motivo, sarebbe meglio evitare di inserire dati sensibili, quali password e numeri di carte di credito.

L'icona rossa con il punto esclamativo indica che il sito in cui ci troviamo non è soltanto poco sicuro, ma addirittura pericoloso. Il browser in questo caso ha individuato seri problemi per la nostra privacy durante la connessione al sito. Il sito, infatti, potrebbe usare tecniche di phishing o trasmetterci malware.

**Attenzione**. Il *phishing* si verifica quando qualcuno assume un'altra identità per indurci a condividere informazioni personali o confidenziali, generalmente tramite un sito web fasullo. Il *malware*, invece, è un software che si installa sui nostri dispositivi senza che ce ne accorgiamo, con lo scopo di danneggiarli o rubare informazioni.

Un'altra cosa da fare per misurare il livello di sicurezza del sito a cui siamo collegati è verificare se per comunicare con il sito stiamo utilizzando il protocollo https (*Hyper Text Transfer Protocol Secure*).

**Nota**. Il protocollo è la prima parte di un indirizzo web (URL). Il protocollo definisce le istruzioni che browser e server utilizzano per comunicare: il browser richiede una determinata risorsa web al server, il quale provvede a fornirgliela. I browser sono in questo modo capaci di visualizzare i contenuti che stiamo cercando.

Il protocollo https è il modo più sicuro per crittografare i dati durante la navigazione in Internet, poiché utilizza il sistema di crittografia SSL (*Secure Sockets Layer*). Questo sistema di crittografia si occupa dell'autenticazione dei dati trasmessi, e pertanto rende la comunicazione tra browser e server più sicura rispetto al normale protocollo http.

A volte può accadere di visitare siti Internet che somigliano in tutto e per tutto a siti più famosi e pertanto considerati sicuri, quando in realtà sono soltanto delle loro imitazioni, creati ad hoc per farci inserire i nostri dati personali e finanziari (questa particolare tecnica di frode si chiama *pharming*).

Per verificare l'autenticità di un sito, possiamo ricorrere al *certificato di sicurezza*. Questo documento elettronico infatti viene rilasciato da un'autorità di certificazione, il cui compito è verificare e accertare l'identità dell'intestatario del sito.

Per verificare l'autenticità del sito web in cui ti trovi, segui questi passaggi:

1. Nella barra degli indirizzi del browser, fai clic sul lucchetto che anticipa l'URL del sito.
2. Nel menu che si apre, seleziona l'opzione *La connessione è sicura*, e subito dopo fai clic su *Il certificato è valido*.

3. Nella finestra di dialogo che si apre, visualizzi le informazioni sul certificato di sicurezza che il sito utilizza per garantire la sua autenticità. In particolare, la voce *Rilasciato a* riporta il nome del titolare del sito. La voce *Rilasciato da* invece riporta il nome dell'ente di certificazione che ha rilasciato il certificato. La validità del certificato è infine limitata. La voce *Valido dal* riporta infatti il periodo di validità del certificato.

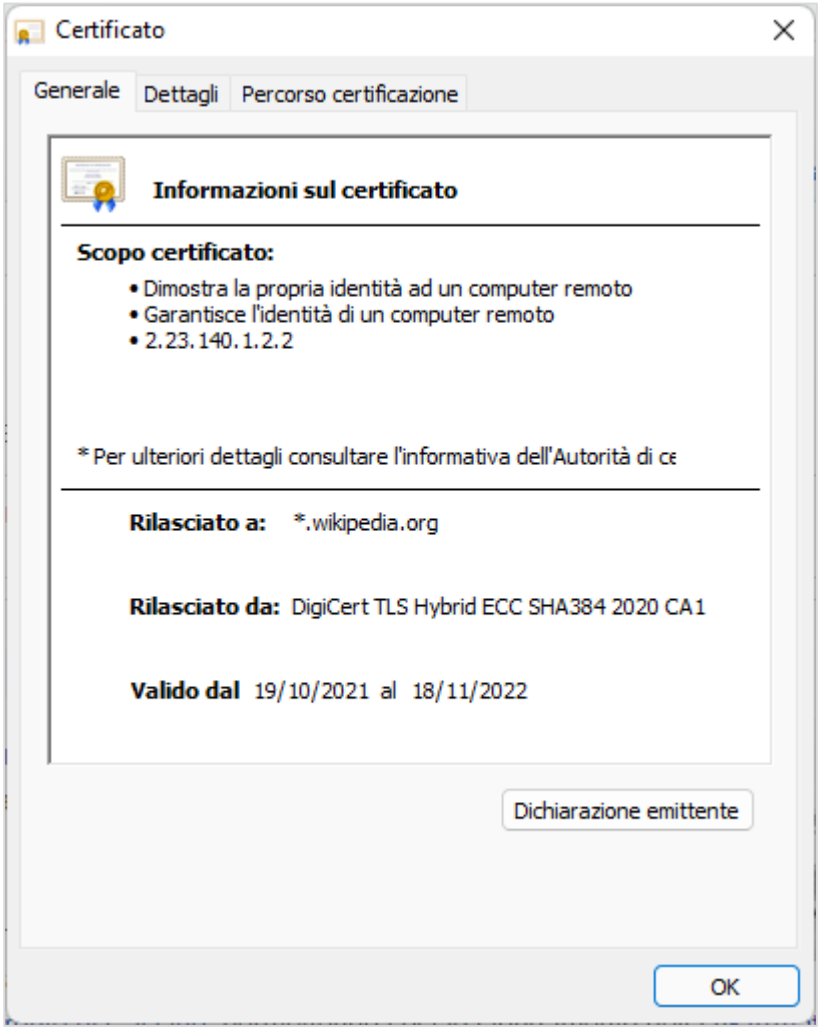



*Figura 4.10 — Il certificato di sicurezza assicura l'autenticità dei siti web che visitiamo*

### 4.2.2. Verificare la sicurezza delle reti wireless

Come abbiamo già detto, per accedere a Internet, possiamo ricorrere a reti wireless private o pubbliche. Alcune di queste reti richiedono una password per accedervi, altre invece sono aperte, e pertanto la connessione può avvenire liberamente.

Le reti wireless che non richiedono una password per accedervi sono più rischiose per la sicurezza degli utenti. Senza una password è infatti più facile per un malintenzionato accedere alla rete wireless, e rubare quindi le informazioni personali di chi è collegato alla rete.

Le reti wireless inoltre utilizzano precisi protocolli di sicurezza per criptare i dati trasmessi nelle comunicazioni (vedi Paragrafo 3.3.3).

In *Windows 11*, una volta che il tuo computer è collegato a una rete wireless, per sapere se questa rete utilizza un adeguato protocollo di sicurezza, segui questi passaggi:

1. Nella barra delle applicazioni, seleziona il pulsante *Start*, quindi fai clic su *Impostazioni*.
2. Nel menu a sinistra della finestra *Impostazioni*, seleziona *Rete e Internet* > *Wi-Fi* > *Proprietà*.
3. La voce *Tipo di sicurezza* riporta il protocollo utilizzato per la connessione alla rete wireless. Verifica dunque che il protocollo sia il *WPA2-Personal*.

Se invece utilizzi un dispositivo mobile *Android* per verificare quale protocollo di sicurezza utilizza la rete wireless a cui sei connesso, segui questi passaggi:

1. Apri l'app *Impostazioni*, quindi seleziona *Connessioni* > *Wi-Fi*.
2. Nella sezione *Reti corrente*, visualizzi il nome della rete wireless a cui sei connesso. Fai dunque tap sull'icona a forma di ingranaggio.
3. La voce *Sicurezza* riporta il tipo di protocollo utilizzato per la connessione alla rete wireless. Verifica dunque che il protocollo sia il *WPA/WPA2-Personal*.

**Suggerimento**. Anche se stai utilizzando una connessione sicura, ricorda di eseguire il *logout* dai tuoi account una volta che hai concluso le operazioni di tuo interesse. Senza eseguire il logout, chi entra in possesso del tuo computer o dispositivo può accedere ai tuoi dati.

### 4.2.3. Utilizzare gli strumenti di filtraggio dei contenuti

Internet è una fonte inesauribile di contenuti. A volte, questi contenuti possono essere inappropriati.

Il motore di ricerca *Google* ci permette di attivare un apposto filtro per escludere dalle ricerche i contenuti più espliciti e inappropriati. Questo filtro si chiama *SafeSearch*, e chiunque disponga di un account *Google* può attivarlo per limitare i risultati delle ricerche su Internet. Il filtro *SafeSearch* non è preciso al 100%, ma consente comunque di escludere dai risultati delle ricerche la maggior parte dei contenuti violenti e per adulti. È molto utile se il nostro computer o dispositivo viene utilizzato da minori.

Per attivare il filtro *SafeSearch* di *Google*:

1. Raggiungi la pagina web *https://www.google.com/safesearch*. Per raggiungere questa pagina web, puoi utilizzare il browser che preferisci (*Chrome*, *Firefox*, *Edge* o *Safari*).
2. Se non lo hai già fatto, accedi al tuo account *Google*.
3. Sposta verso destra la barra in corrispondenza dell'opzione *Filtro per risultati espliciti*.

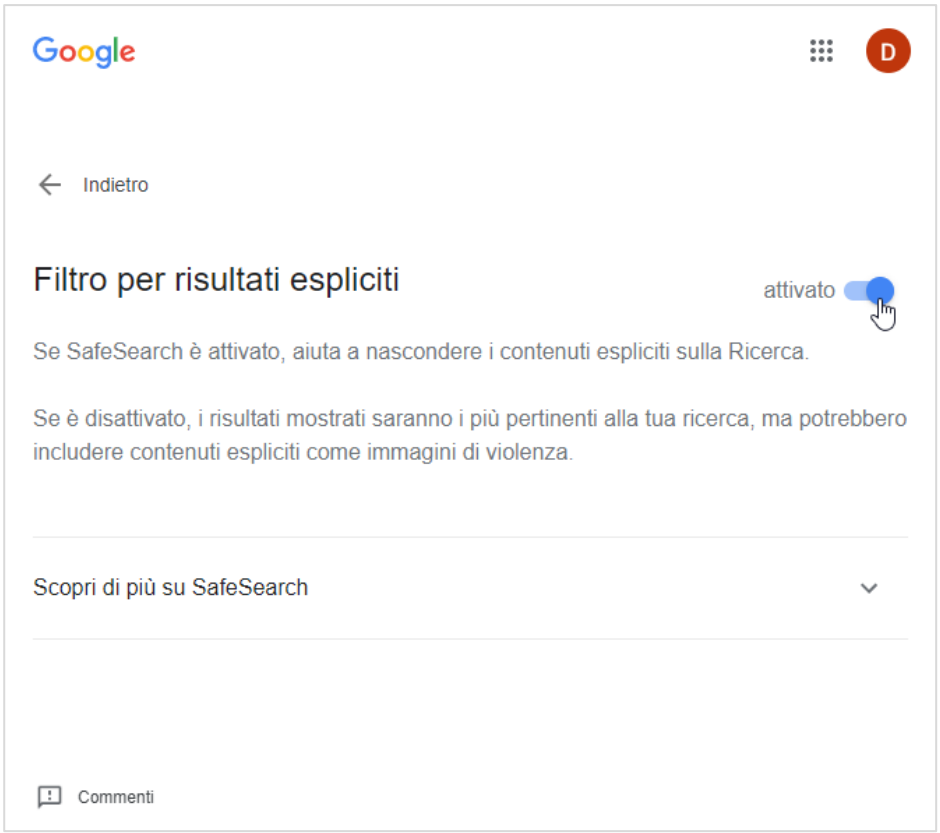



*Figura 4.11 — Attivare il filtro SafeSearch di Google*

# 5. Sicurezza nelle comunicazioni online

## 5.1. Posta elettronica

La posta elettronica è uno dei servizi online che con il tempo si è diffuso maggiormente. Oggi è diventato uno strumento di lavoro e di comunicazione pressoché indispensabile per milioni di utenti in tutto il mondo.

Benché la maggior parte degli utenti si connetta ai server di posta elettronica in maniera sicura, è possibile che estranei malintenzionati riescano comunque a intercettare, leggere e alterare le email durante il percorso che dal mittente le porta al destinatario.

**Nota**. La posta elettronica utilizza un sottoinsieme della rete Internet diverso dal World Wide Web, chiamato Mail_To. Il carattere chiocciola (@), presente pressoché in ogni indirizzo email, indica che l'indirizzo si riferisce proprio al Mail_To. I server che gestiscono i contenuti del web sono in questo modo capaci di riconoscere gli indirizzi che riguardano la comunicazione via email, e possono pertanto separare questa attività dal resto delle funzionalità legate al Web.

### 5.1.1. La cifratura come argine alle infiltrazioni malware

Anche se per accedere al nostro account di posta elettronica dobbiamo eseguire il login, è possibile che le email che inviamo e riceviamo non siano al sicuro.

Nella maggior parte dei casi infatti le email vengono trasmesse in chiaro, ossia senza alcun sistema di cifratura che impedisca a un malintenzionato — il così detto *Man in the middle* — di intercettarle e leggerle.

I messaggi di posta elettronica trasmessi in chiaro sono come lettere inviate in buste aperte, che tutti possono leggere. La crittografia invece ci permette di nascondere a terze persone il contenuto delle nostre email, visto che con la crittografia soltanto i destinatari delle email hanno le chiavi per decodificarle.

Per mettere al sicuro i nostri messaggi di posta elettronica possiamo dunque crittografarli, e per fare ciò, possiamo ricorrere a specifici servizi online, come *Virtru*, *ProtonMail*, *Lockbin*.

In questo modo, se qualcuno dovesse interporsi tra l'invio e la ricezione dei messaggi, non sarà comunque in grado di decifrare i contenuti delle nostre comunicazioni.

**Suggerimento**. La maggior parte dei software dannosi che attaccano i nostri computer provengono dagli allegati alle email che riceviamo. È dunque di importanza fondamentale scansionare tutti gli allegati con un antivirus prima di aprirli, soprattutto se provengono da mittenti sconosciuti. Se le email che riceviamo ci sembrano sospette, sarebbe meglio evitare di aprirle. Un'altra soluzione per tenere al sicuro le nostre email, è scegliere una password complessa per accedere alla nostra casella di posta elettronica, e cambiarla di frequente.

### 5.1.2. La firma digitale come sistema per identificare il mittente delle email

La firma digitale garantisce l'identità del mittente di un messaggio di posta elettronica. In pratica la firma digitale è l'equivalente di una firma autografata in modo tradizionale.

Con l'apposizione della firma digitale qualsiasi documento informatico acquisisce, a tutti gli effetti, valore legale. Proprio per questo motivo, è diventata negli ultimi anni sempre più diffusa.

La firma digitale viene rilasciata da specifici soggetti pubblici o privati, i quali sono stati legalmente autorizzati a svolgere servizi di autenticazione.

Dal punto di vista tecnico, la firma digitale utilizza uno tra i più sicuri sistemi di cifratura dei dati, il così detto *sistema di cifratura a doppia chiave asimmetrica*. In pratica, per cifrare i dati, questo sistema utilizza una coppia di chiavi crittografiche — una privata e una pubblica.

Ad ogni chiave privata corrisponde una sola chiave pubblica. La chiave privata è usata per generare la firma digitale da apporre al documento elettronico, mentre la chiave pubblica è usata per verificare l'identità di chi appone la firma digitale.

Questo metodo garantisce la piena sicurezza visto che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata, e il destinatario avrà la certezza dell'identità del mittente.

Con la firma digitale vengono rispettati i seguenti principi.

- *Validità legale*. Il documento firmato digitalmente acquisisce pieno valore legale.

- *Autenticità*. L'identità di chi sottoscrive il documento è garantita.
- *Integrità*. L'inalterabilità del documento sottoscritto è assicurata.
- *Non ripudio*. Il documento firmato non può essere disconosciuto dal firmatario.

### 5.1.3. Riconoscere lo spam

Lo *spam* è un disturbo alla nostra comunicazione online, arrecato da terzi mediante l'invio di messaggi di posta elettronica non richiesti.

L'obiettivo degli *spammer* (ossia, degli hacker che compiono attività di spam) è quello di carpire i nostri dati personali, come numeri di carte di credito o di conto corrente, e di conoscere le credenziali di accesso ai nostri account. Ogni informazione personale è un dato utile per chi fa spam.

Di solito, i messaggi spam contengono pubblicità. Oltre a comuni offerte commerciali, i messaggi spam possono proporci l'acquisito di materiale pornografico, di farmaci senza prescrizione medica o che provengono dall'estero, di prodotti contraffatti o illegali, ecc.

In alcune occasioni, invece, i messaggi spam sono delle vere e proprie truffe, visto che ci propongono operazioni finanziarie molto vantaggiose, capaci cioè di generare notevoli guadagni in poco tempo, o che ci comunicano di aver vinto una grande cifra, e che per riscuoterla, dobbiamo inserire i nostri dati personali.

A volte gli hacker possono spingersi oltre, arrivando a pubblicare falsi siti web, in cui — per attirare più persone possibili —, promettono vantaggi e offerte sorprendenti. I malcapitati sono dunque attratti da queste facili opportunità, e pur di beneficiarne, sono disposti a lasciare il loro indirizzo di posta elettronica e i loro dati personali.

I provider utilizzano specifici sistemi di filtraggio della posta elettronica per arginare lo spam, ma nonostante ciò, lo spam continua a imperversare sul Web. La soluzione per evitare di esserne vittime è dunque adottare precisi comportamenti.

Per prima cosa, dovremmo essere molto attenti quando condividiamo il nostro indirizzo email. Se ad esempio gestiamo un blog, scriviamo su un forum o su un gruppo di discussione (newsgroup), o più semplicemente, se abbiamo un profilo social, sarebbe

meglio evitare di pubblicare il nostro indirizzo di posta elettronica, a meno che non vogliamo essere contattati in privato dagli altri utenti. Gli spammer infatti utilizzano specifici programmi per copiare automaticamente gli indirizzi email dal Web.

Dovremmo inoltre evitare di rispondere ai messaggi di posta elettronica che sospettiamo possano contenere spam. Come abbiamo già detto, i provider adottano soluzioni tecniche per limitare lo spam, ma nonostante ciò, può accadere che qualche messaggio fraudolento possa comunque arrivare nelle nostre caselle di posta elettronica. In questi casi, dobbiamo evitare di compiere qualsiasi tipo di azione che ci viene richiesta nel messaggio. Dobbiamo inoltre evitare di rispondere al messaggio per dire che non siamo interessati, o che intendiamo procedere legalmente, visto il tentativo di ingannarci. Queste azioni infatti non fanno altro che confermare agli spammer di aver raggiunto un indirizzo di posta elettronica valido, al quale cioè corrisponde realmente una persona, e che pertanto può costituire un buon obiettivo per le loro manovre illecite.

Uno dei trucchi più utilizzati dagli spammer per indurci a rispondere alle loro email fraudolente (in modo da verificare se il nostro indirizzo di posta elettronica potrebbe essere un valido bersaglio) è quello di inserire nei messaggi false opzioni di cancellazione, del tipo: *Se non vuoi ricevere altre email da noi, clicca qui*. In questi casi, dovremmo sempre evitare di rispondere.

Come abbiamo visto nel paragrafo 4.1.2, i browser ci permettono di memorizzare i nostri dati personali, in modo da poterli inserire in automatico ogni volta che, ad esempio, creiamo un account o facciamo un acquisto da un sito di e-commerce. Questa funzione, con la quale possiamo completare un modulo online in una sola mossa, è molto comoda e ci permette di risparmiare tempo. Dall'altro lato però mette a rischio la sicurezza dei nostri dati personali, visto che è una tra le funzioni più attaccabili dagli spammer, e da tutti quelli che sono alla ricerca di indirizzi email da bersagliare con messaggi spam.

Un'ultima soluzione per evitare lo spam è quella di fare attenzione all'informativa sulla privacy, soprattutto quando utilizziamo un servizio online (facciamo un acquisito ad esempio). In questo caso, dobbiamo verificare se l'informativa sulla privacy prevede la divulgazione del nostro indirizzo di posta elettronica ad altre aziende partner. In molte occasioni, possiamo scegliere se lasciare questa libertà o meno a chi gestisce il sito.

### 5.1.4. Riconoscere il phishing

Il *phishing* è una particolare tecnica di frode, con la quale gli hacker riescono a raccogliere le informazioni personali di chi viene ingannato. In pratica, gli hacker inviano alle loro vittime messaggi di posta elettronica soltanto in apparenza veritieri. Alle potenziali vittime può infatti sembrare che questi messaggi provengano da banche, fornitori di servizi a pagamento o negozi online. I messaggi inoltre esortano le vittime a cliccare su un link per avere maggiori dettagli su ciò che il messaggio propone. In questo modo, i malcapitati finiscono per collegarsi a siti web creati ad hoc per rubare le loro informazioni personali.

Con questi attacchi informatici, gli hacker vogliono rubare username, password, numeri di carte di credito, e qualsiasi altro tipo di dato personale, in modo da fare prenotazioni o acquisti a spese delle loro vittime.

Generalmente, le email di phishing ci chiedono di fornire:

- Nomi utente e password, incluse le modifiche delle password
- Codici fiscali
- Numeri di conti bancari
- PIN (*Personal Identification Number*)
- Numeri di carte di credito
- La nostra data di nascita

Con un po' di attenzione, possiamo rilevare facilmente un tentativo di phishing. Ecco alcuni elementi da tenere sott'occhio per riconoscerlo:

- Se il mittente di una email da noi ricevuta è una banca, un ente pubblico o una grossa azienda, sarebbe meglio verificare se siamo già entrati in contatto con queste società, e se abbiamo fornito loro il nostro indirizzo di posta elettronica. Verifichiamo dunque l'intero indirizzo web del mittente, e confrontiamolo con le email che potrebbe averci inviato in precedenza.
- Di solito le aziende si rivolgono ai loro clienti chiamandoli per nome. La stessa cosa accade quando è un ente pubblico a voler comunicare con i cittadini. Gli hacker di solito non dispongono del nome completo delle loro vittime, e pertanto le email

ingannevoli con cui cercano di raggirarle utilizzano formule impersonali, come ad esempio *Gentili signori* o *Gentili signore*. Quando ci accorgiamo che una email è poco attenta a questi particolari, ci conviene diffidare di ciò che riporta.

- Se il testo di una email è pieno di errori ortografici e grammaticali, è molto probabile che si tratti di una truffa. Gli errori di questo tipo, insieme alle informazioni spiegate in modo troppo contorto, sono infatti un chiaro indizio che si tratti di un tentativo di phishing. Gli hacker infatti non perdono tempo a tradurre correttamente i testi delle loro email ingannevoli, che magari sono state scritte prima in una lingua, e poi tradotte in un'altra, senza fare alcuna attenzione alla correttezza del testo.
- Se un messaggio di posta elettronica contiene un link, prima di cliccarci sopra per aprirlo, sarebbe meglio verificarlo. Per fare ciò, è sufficiente posizionare il cursore sul link, in modo da visualizzare l'URL del link nella barra inferiore della finestra del browser. A questo punto, possiamo controllare se l'URL coincide con quello che ci aspettavamo (visto il contenuto del messaggio e l'identità del mittente), e se per la trasmissione dei dati vengono utilizzati protocolli http di sicurezza. Se abbiamo dei dubbi, evitiamo di aprire il link, o di inserire il suo URL nella barra degli indirizzi del browser.
- Nessun negozio online chiede ai suoi clienti di trasmettere dati personali tramite email. Se in un messaggio di posta elettronica ci viene chiesto di compilare un form, possiamo stare certi che si tratta di un tentativo di *phishing*.
- Se una email contiene un invito all'azione immediata è necessario prestare molta attenzione. I truffatori a volte usano le maniere forti per mettere sotto pressione gli utenti e spingerli ad azioni avventate. Il punto è che nessuna azienda minaccia un blocco della carta di credito o il ricorso a un'agenzia di recupero crediti, costringendo così a inserire una password o a scaricare un allegato. Nel dubbio, chiamiamo l'assistenza clienti del mittente.

In conclusione, è bene ricordare che nessuna azienda seria invia email ai suoi clienti per chiedere loro informazioni personali. Ciò significa che non bisogna mai rispondere alle email che ci chiedono di inserire i nostri dati personali.

### 5.1.5. Che cosa fare in caso di phishing

Quando riceviamo un email dannosa, la prima operazione da compiere è spostarla nella cartella *Spam* della nostra casella di posta elettronica.

**Nota**. La cartella in cui raccogliere le email dannose può cambiare nome in base al servizio di posta elettronica da noi utilizzato. Nel servizio di posta elettronica *Gmail* di *Google*, questa cartella si chiama *Spam*, nell'applicazione *Posta* di Windows 11, con la quale gestire la posta elettronica, questa cartella si chiama *Posta indesiderata*.

Nel servizio di posta elettronica *Google Gmail*, per spostare una email nella cartella *Spam*, segui questi semplici passaggi:

1. Nella cartella *Posta in arrivo*, seleziona la email da spostare nello Spam.
2. Nella barra al di sopra della email, seleziona il pulsante *Segnala come Spam* 

Fatto ciò, ti conviene bloccare il mittente della email fraudolenta, in modo da impedirgli di continuare a inviarti altre email. In *Gmail*:

1. Apri il messaggio di posta elettronica che costituisce l'attacco di phishing.
2. Nella sezione in alto a destra dell'intestazione della email, seleziona il pulsante *Altro*. L'icona di questo pulsante è costituita da tre puntini verticali.
3. Nel menu che si apre, seleziona l'opzione *Blocca*, seguita dal nome del mittente del messaggio fraudolento.

Quando un messaggio costituisce un attacco di phishing, puoi segnalarlo al team antifrode di *Google*, per aiutarlo a sventare questo e altri attacchi.

1. Nel menu che si apre dopo aver selezionato il pulsante *Altro* (vedi il punto 2 della procedura qui sopra), seleziona l'opzione *Segnala phishing*.
2. Nella finestra di dialogo che si apre, seleziona il pulsante *Segnala messaggio phishing*.

Sarebbe inoltre utile segnalare le email che contengono phishing alle organizzazioni legittime (vale a dire, la vera banca, il vero sito di e-commerce, il vero ente istituzionale, ecc.). Nel phishing infatti il mittente del messaggio fraudolento si finge rappresentante di

un'organizzazione legittima, per cercare di truffare il destinatario, e portarlo a divulgare alcune sue informazioni personali, come ad esempio una password, o il numero di una carta di pagamento.

Quando non siamo riusciti a evitare il tentativo di phishing, dobbiamo intervenire in un altro modo. Non possiamo limitarci a isolare la email fraudolenta, bloccare il mittente, e segnalarla alle organizzazioni legittime. Se ci accorgiamo ad esempio che sul nostro conto corrente avvengono movimenti che non ricordiamo di aver autorizzato, dobbiamo subito contattare il servizio clienti della nostra banca, e chiedere di bloccare immediatamente la nostra carta di pagamento. In questi casi, dobbiamo anche sporgere denuncia alla Polizia.

## 5.2. Reti sociali

Le reti sociali sono gruppi di persone connesse tra loro da qualsiasi legame di tipo sociale. In quanto animali sociali, noi tutti viviamo da sempre all'interno di queste reti.

Nel tempo, il concetto sociologico di rete sociale si è saldato sempre di più con lo sviluppo tecnologico, tanto da aver contribuito alla definizione dei così detti *social network*, o più semplicemente *social*. L'espressione *social network* infatti indica gli strumenti tecnologici con cui possiamo entrare in relazione virtualmente con altre persone.

Nell'ultimo ventennio, infatti, l'innovazione tecnologica ha consentito la creazione di specifiche piattaforme informatiche, con le quali possiamo diventare parte di reti sociali molto estese, le cui dimensioni hanno ormai raggiunto intere aree del globo. Persone di nazionalità diversa e fisicamente molto lontane tra di loro, grazie a queste piattaforme online, possono entrare in contatto l'una con l'altra, e costituire così una comunità virtuale

Ad oggi, il social network più conosciuto e utilizzato al mondo è *Facebook*. Anche *Instagram* e *Tik Tok* vengono utilizzati sempre di più, soprattutto dai giovanissimi. Ci sono poi una serie di social network, nati con lo scopo di soddisfare esigenze specifiche, come *LinkedIn*, con cui è possibile entrare in contatto con altre persone per motivi professionali.

I social vogliono agevolare i legami che possono instaurarsi tra le persone, e pertanto chiedono a ciascun componente della comunità di fornire diverse informazioni personali, come ad esempio i propri interessi, il proprio lavoro e i propri hobby. Queste informazioni

infatti possano aiutare gli altri componenti della comunità virtuale a identificare meglio chi noi siamo, e così facendo, i social creano comunità di persone più o meno simili, unite dalla reciproca somiglianza.

### 5.2.1. La sicurezza nelle reti sociali

I social non hanno soltanto vantaggi. Il loro utilizzo infatti ha dei risvolti negativi. I social possono mettere a rischio la nostra sicurezza online, ed è molto comune che si verifichino furti di identità. Ci sono dunque precise norme di condotta da osservare mentre operiamo sui social network.

Per partecipare a qualsiasi social network, come ad esempio *Facebook*, è necessario creare un *profilo*, in cui inserire i propri dati personali. Normalmente, un profilo richiede di inserire il proprio nome, un'immagine che ci rappresenti e un indirizzo di posta elettronica a cui essere rintracciati.

Nel momento in cui creiamo il nostro profilo in una rete sociale, è come se stessimo diventando personaggi pubblici, certamente di poca rilevanza, almeno all'inizio. La cosa da tenere in considerazione però è che una volta entrati nella comunità virtuale di una rete sociale, siamo tutti in qualche modo costretti a fare attenzione alla nostra esposizione pubblica. Il nostro profilo, infatti, come quello di molti, è visibile a tutti (o quasi tutti) gli altri componenti della comunità. Occorre dunque utilizzare una buona dose di prudenza.

In generale, quando pubblichiamo foto o immagini personali che ritraggono sia noi che gli altri, dovremmo sempre avere molta accortezza, perché sono informazioni che stiamo condividendo con altre persone, anche se con qualche limitazione.

Le informazioni personali che non andrebbero mai condivise sulle reti sociali sono le foto o immagini che ritraggono gli spazi in cui si svolge la nostra vita, come ad esempio, la nostra abitazione, scuola o azienda. Queste informazioni infatti se diffuse senza prestare le dovute attenzioni possono costituire un pericolo.

Non va mai dimenticata la "memoria" del Web: ciò che viene messo online rimane online. Sarebbe pertanto meglio evitare di pubblicare contenuti che in futuro potrebbero metterci in imbarazzo. Prima di condividere qualcosa, bisogna riflettere con attenzione, poiché il

materiale pubblicato sul Web è permanente, e qualcuno in futuro potrebbe utilizzarlo contro di noi. Chiunque, ad esempio, può stampare facilmente un articolo che abbiamo pubblicato su un blog, e salvarlo per sempre sul suo computer.

In definitiva, sarebbe davvero ingenuo credere che l'utilizzo dei social network non comporti gravi rischi per la nostra sicurezza. I nostri contenuti personali sono potenzialmente visibili a tutto il mondo, e una volta condivisi, non possiamo più cancellarli. Vengono infatti archiviati nei server della società che gestisce la comunità online a cui partecipiamo, secondo quanto disposto dalle norme vigenti. Ciò avviene perché le autorità giudiziarie devono poter accedere a queste informazioni qualora dovessero ritenerlo necessario per l'esercizio delle loro funzioni.

Dobbiamo infine considerare il rischio di dover rispondere anche legalmente per aver diffuso informazioni false o diffamatorie, per aver promosso idee o azioni illegali, o per aver diffuso materiale protetto da copyright o dannoso.

### 5.2.2. La privacy nelle reti sociali

Visto che le reti sociali ci espongono in un contesto pubblico che non sempre possiamo controllare completamente, la prima regola da osservare per preservare la nostra privacy, insieme a quella delle persone a noi vicine, è quella di evitare di rendere pubbliche informazioni personali, che malintenzionati potrebbero utilizzare per scopi ingannevoli.

Oltre ai dati obbligatori che ci vengono richiesti quando creiamo il nostro profilo, sarebbe meglio evitare di fornire altre informazioni personali. Di solito, i profili nelle reti sociali sono pubblici, nel senso che ogni componente della comunità virtuale può visualizzarli. Come sistema di protezione della nostra identità sarebbe meglio limitare la possibilità di accedere ai nostri dati personali soltanto alle persone che conosciamo nella vita reale, e che pertanto fanno parte della nostra cerchia di amici.

La semplicità con cui instauriamo legami sui social rende estremamente facile confondere la sfera privata con quella pubblica. A tal proposito, è controproducente mostrarsi sui social in modo diverso da come si è realmente. Per quanto ciascuno di noi cerchi in qualche modo di adattarsi ai contesti sociali in cui opera, è bene ricordare che presto o tardi la

discrepanza tra ciò che mostriamo di essere e ciò che invece siamo nella vita di tutti i giorni può causarci qualche problema. Tutto questo contribuisce a rendere la parola online più carica di significato, e soprattutto più carica di conseguenze.

Ogni nostra pubblicazione sul Web inoltre può diventare oggetto di studio e analisi. Sono molti coloro che, a seconda dei casi, sono o possono essere interessati a conoscerci meglio. Di solito, quando ci iscriviamo a un social, tra le condizioni che accettiamo (nella maggior parte dei casi, senza mai leggerle) c'è il consenso, rilasciato alla società che gestisce la comunità online, di trasferire i nostri dati personali a terzi per finalità statistiche, o molto più spesso, commerciali. Anche se decidessimo di cancellare il nostro account, questi dati resterebbero disponibili e utilizzabili sia dal gestore della comunità online che da terzi. In casi del genere, è certo che riceveremo proposte commerciali che non abbiamo richiesto, anche dopo che avremo eventualmente chiuso il nostro profilo.

Anche dal punto di vista professionale i social andrebbero utilizzati con attenzione. Le aziende a cui abbiamo inviato il nostro curriculum infatti potrebbero utilizzare i social per avere più informazioni su di noi, prima di contattarci per un eventuale colloquio. Essere cauti nell'esprimere le proprie opinioni politiche, religiose o sessuali, è dunque fondamentale quando si interagisce con altre persone sui social network. La riservatezza resta in ogni occasione il comportamento migliore da adottare.

Se è vero che ognuno di noi è libero di esprimere le sue opinioni politiche, religiose o sessuali, è altrettanto vero che anche i governi occidentali hanno cominciato ad acquisire dai social le informazioni che ritengono possano essere utili per arginare fenomeni come, ad esempio, quello terroristico. La cronaca di tutti i giorni racconta come arresti ed espulsioni siano sempre di più la conseguenza di esternazioni fatte e acquisite sui social.

### 5.2.3. Configurare le impostazioni sulla privacy

Tutti i social dispongono di una ampia sezione dalla quale possiamo configurare la privacy del nostro profilo, in modo da specificare chi e cosa potrà visualizzare quello che pubblichiamo. In linea di massima è importante evitare di rendere pubblica ogni nostra attività sui social, ma soprattutto prendere la buona abitudine di rivedere, di tanto in tanto, le nostre impostazioni sulla privacy.

Prendiamo in considerazione *Facebook*, e vediamo come configurare le impostazioni sulla privacy.

1. Esegui il login per accedere alla home page di *Facebook*.
2. Nell'area a destra della barra superiore, fai clic sul pulsante con una freccia verso il basso.
3. Nel menu che si apre, seleziona *Impostazioni e privacy* > *Controllo della privacy*.
4. Il *Controllo della privacy* è la sezione di *Facebook* che ti guida attraverso alcune delle impostazioni di protezione e privacy, in modo che tu possa controllare le tue scelte per assicurarti di condividere le informazioni con chi desideri.

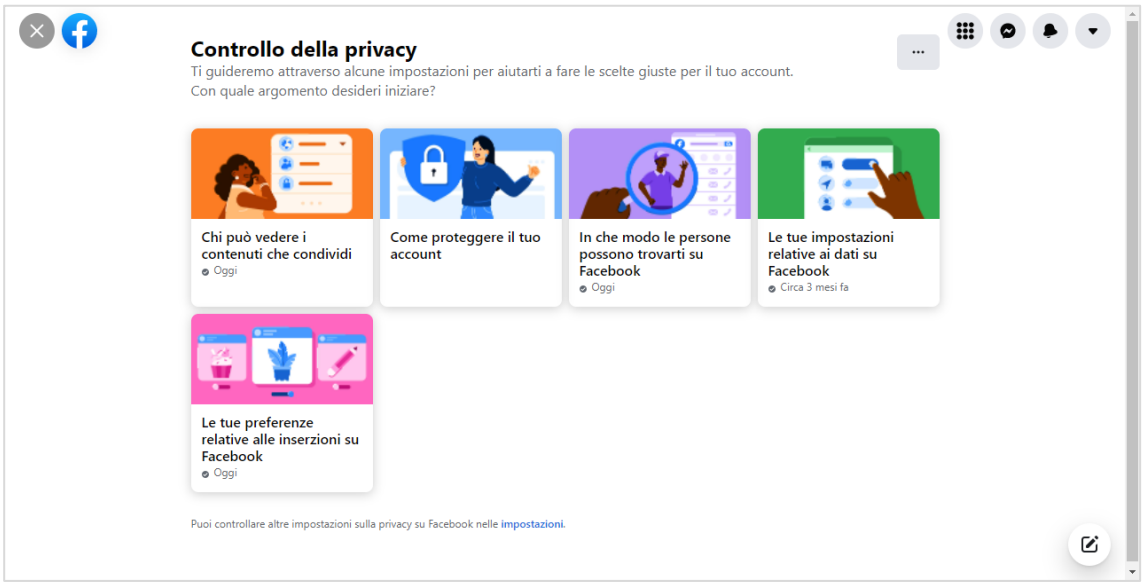



*Figura 5.1 — La pagina di Facebook da cui configurare le impostazioni per la privacy*

È importante riesaminare periodicamente le proprie impostazioni sulla privacy. A volte infatti i social network possono modificare e arricchire queste impostazioni.

*Facebook* ad esempio ci dà la possibilità di configurare un promemoria, in modo da ricordarci di verificare le impostazioni sulla privacy del nostro profilo.

Per programmare questo promemoria, accedi alla sezione di *Facebook* da cui eseguire il controllo della privacy (vedi la Figura 5.1), quindi fai clic sul pulsante con tre puntini orizzontali (vedi la Figura 5.2). Nel menu che si apre, seleziona l'opzione *Configura promemoria*.

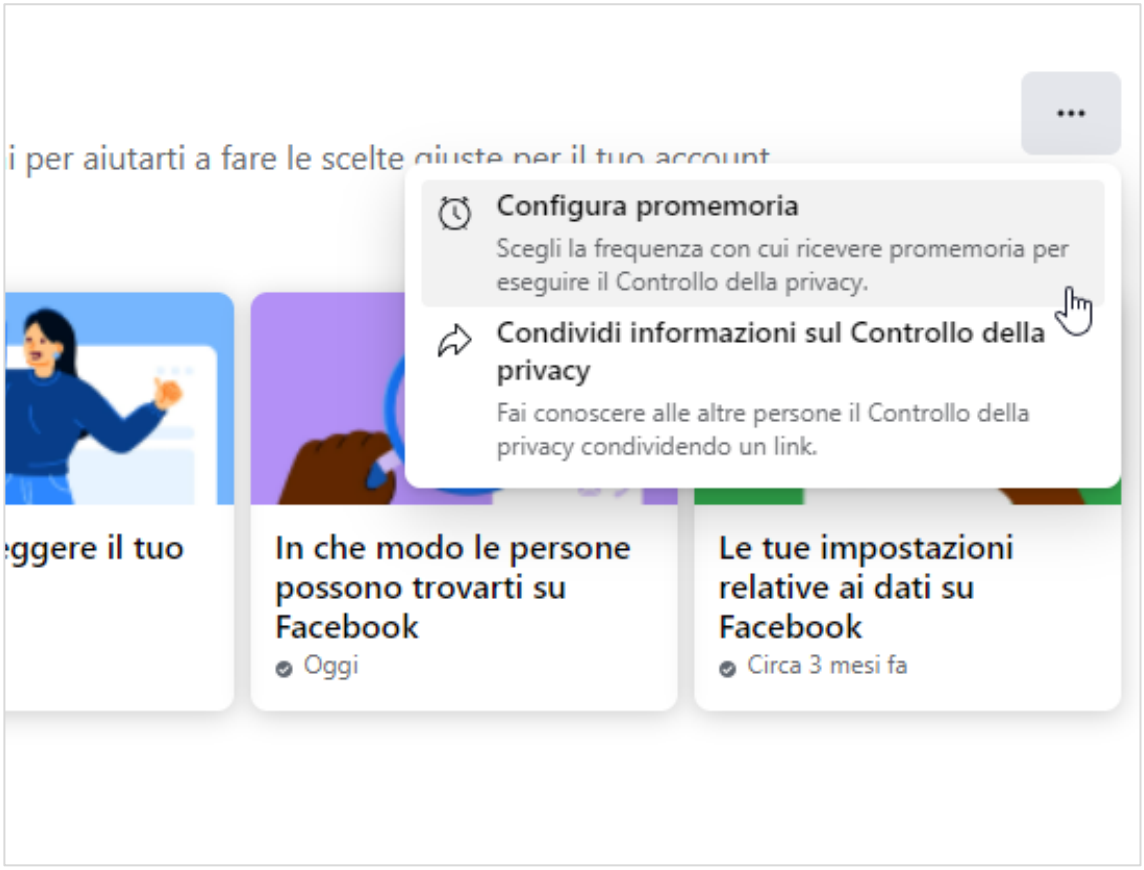



*Figura 5.2 — Ricevere un promemoria per verificare le impostazioni sulla privacy del proprio profilo Facebook*

La finestra di dialogo che compare mostra le opzioni a tua disposizione per scegliere la frequenza con cui ricevere il promemoria (*Ogni settimana*, *Ogni mese*, *Ogni 6 mesi* e *Ogni anno*). Scegli dunque l'opzione che preferisci, dopodiché fai clic sul pulsante *Salva*.

Per avere maggiori informazioni su ogni aspetto della privacy, fai clic sul pulsante con una freccia verso il basso nell'area a destra della barra superiore della home page di *Facebook*, e nel menu che si apre, seleziona *Impostazioni e privacy* > *Centro sulla privacy*.

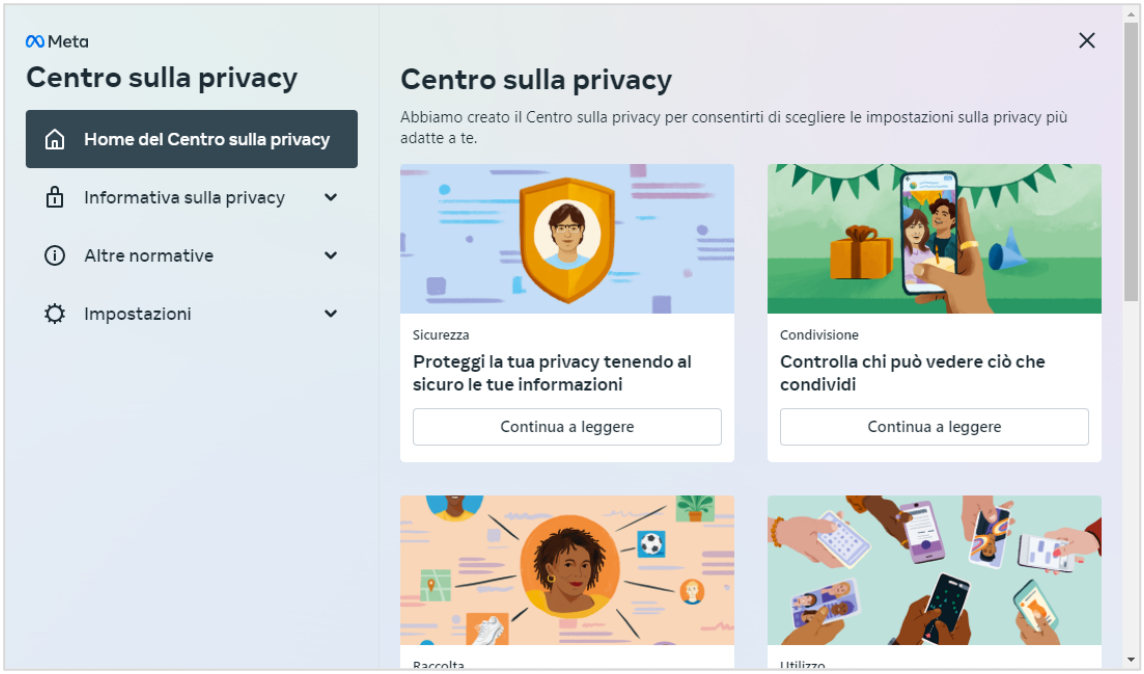



*Figura 5.3 — Il Centro sulla privacy di Facebook*

### 5.2.4. I rischi della comunicazione sulle reti sociali

Una minaccia particolarmente diffusa nelle reti sociali è il *Social network poisoning*, con cui gli hacker creano profili artefatti e relazioni inesistenti per contraffare e rendere inaffidabili le informazioni che i componenti delle comunità online condividono quotidianamente.

Non essendo possibile verificare sempre e in ogni momento la veridicità dei profili, è possibile imbattersi in utenti parzialmente o completamente falsi (si parla, in casi del genere, di *fake*). I principali casi di *poisoning* attualmente praticati sono la sostituzione e la simulazione di identità; l'introduzione volontaria di elementi falsi o non congrui nel proprio profilo; e l'ingresso in gruppi che non hanno nulla a che fare con i nostri interessi e relazioni, con il solo intento di fare rumore.

I social network vengono spesso utilizzati per fare disinformazione. Le notizie false — le così dette *fake news* — sono informazioni false o in parte corrispondenti al vero, che vengono diffuse intenzionalmente sui mezzi di comunicazione di massa, tra cui i social network, per influenzare l'opinione pubblica, tanto da orientarne le scelte e le idee.

Molto spesso le fake news vogliono spingere i lettori a condividerle con altre persone, in modo da innescare un meccanismo che porti ad amplificarle.

La diffusione di fake news è un fenomeno che esiste da moltissimi anni. Già dall'antichità si è infatti cercato di influenzare le persone e le loro opinioni attraverso la diffusione di notizie false. Nel mondo contemporaneo, la digitalizzazione e i social network hanno semplicemente acuito questo fenomeno, tanto da spingere le autorità governative a organizzare vere e proprie campagne contro la disinformazione.

Le fake news riguardano ormai tutti gli ambiti dell'attualità, dalle guerre alle pandemie, dai cambiamenti climatici ai flussi migratori, dai diritti umani alle elezioni politiche, dagli andamenti dei mercati finanziari alle scoperte scientifiche.

A prima vista, le fake news assomigliano a notizie attendibili, che sono state verificate prima della loro pubblicazione. In realtà, sono soltanto notizie create ad hoc, con l'intento di seminare dubbi, sminuire tesi elaborate da istituzioni autorevoli, o promuovere teorie complottiste.

Questo fenomeno è particolarmente problematico al giorno d'oggi, visto che i social network stanno sempre più sostituendo i classici media come giornali, radio, televisione o siti di notizie governativi.

Individuare informazioni false non è sempre facile. Ecco alcuni indizi per riconoscerle.

- La prima cosa da controllare per riconoscere le fake news è l'URL della pagina web in cui le notizie vengono riportate. Molto spesso, gli URL delle pagine web in cui vengono pubblicate fake news sono simili a quelli che rimandano a pagine web già esistenti, e possono diversificarsi dagli URL originali soltanto di qualche carattere o lettera.
- Un'altra cosa da controllare è se le fonti da cui provengono le notizie sono attendibili. In questo caso, le domande che ci dobbiamo porre sono del tipo: "Chi ha scritto la notizia, il post o l'articolo?", "Qual è l'ente o istituto che l'ha pubblicata?", "La notizia è stata riportata in modo neutrale, oppure è stata riportata in modo da difendere e sostenere una tesi in particolare?".
- Anche l'aspetto grafico delle pagine web in cui le notizie vengono riportate può essere una spia, alla quale fare attenzione per comprendere se si tratta di una fake news. Di solito, i siti web con cui le fake news vengono diffuse utilizzano formati

poco professionali, ed è facile che i testi presentino errori di battitura, o più in generale, siano poco curati anche per come le informazioni vengono spiegate.

- La comunicazione sul web tiene molto in considerazione i titoli dei testi, soprattutto quando si tratta di diffondere notizie sui social network, in cui si cerca di catturare al più presto l'attenzione degli utenti. Molto spesso i titoli vengono scelti non tanto per informare sinteticamente di cosa tratta l'articolo, il post o la notizia, ma vengono elaborati con lo scopo di spingere gli utenti del social a entrare nella pagina web che riporta la notizia. Si tratta in sintesi di "titoli esca", che fanno leva sull'emotività soggettiva, e che pertanto utilizzano toni sensazionalistici, paradossali ed enfatici, per attirare l'attenzione di chi li legge. Dal punto di vista grafico è facile riconoscere titoli di questo tipo. Di solito, vengono scritti in maiuscolo, e contengono punti esclamativi o interrogativi. Perciò, se un titolo ha queste caratteristiche, è molto probabile che introduca informazioni false o faziose.
- Come i titoli, anche le immagini vengono spesso utilizzate per catturare l'attenzione degli utenti dei social network. Le fake news infatti possono contenere immagini ritoccate, o addirittura finte. Alcune volte invece le immagini sono autentiche, soltanto che vengono prese fuori dal loro contesto, e utilizzate per sostenere una tesi infondata o poco credibile. Per verificare l'origine delle immagini che circolano sul Web, possiamo utilizzare il sito *TinEye*, ad esempio, ed eseguire quella che viene chiamata "ricerca inversa". In pratica, possiamo utilizzare l'URL dell'immagine per verificarne la fonte.
- Le notizie che troviamo sul Web e che vengono condivise sui social possono riferirsi a fatti accaduti già da diverso tempo. È bene dunque controllare sempre la data di pubblicazione delle notizie, in modo da poter valutare se sono state pubblicate con il solo intento di attirare la nostra attenzione, e se invece sono state pubblicate per informarci. Anche la cronologia degli eventi raccontati nelle fake news potrebbe seguire un ordine sbagliato. Le fake news infatti creano finte argomentazioni pur di sostenere opinioni personali.

Se quando siamo davanti a una notizia abbiamo qualche dubbio sulla sua plausibilità, possiamo eseguire una semplice operazione, ossia cercarla con *Google*. In alternativa,

possiamo verificarne l'attendibilità su siti specializzati nello scovare fake news, come il portale www.*bufale.net*, *www.bufalopedia.blogspot.com* e *www.butac.it*

## 5.3. Messaggistica istantanea

La messaggistica istantanea è un servizio con cui possiamo inviare e ricevere messaggi in tempo reale. Per usufruire di questo servizio, occorre collegarsi a Internet, e disporre delle applicazioni per inviare e ricevere i messaggi.

I servizi di messaggistica istantanea sono tra i sistemi di comunicazione più diffusi al giorno d'oggi, tanto da venire utilizzati anche nelle comunicazioni aziendali, in alternativa alle email.

Servizi di messaggistica istantanea molto diffusi sono *Whatsapp*, *Telegram*, *Messenger*, *WeChat*.

**Nota**. In alcune occasioni, i servizi di messaggistica istantanea sono inclusi in altre applicazioni con cui possiamo eseguire chiamate tramite Internet. Si tratta delle applicazioni VoIP, (*Voice over IP*, ovvero "voce tramite protocollo Internet"), le quali sono sempre più diffuse al giorno d'oggi, dato che permettono di risparmiare notevolmente sui costi delle chiamate rispetto ai sistemi tradizionali. Un'applicazione VoIP attualmente tra le più diffuse è *Skype*, inclusa nelle ultime versioni del sistema operativo *Windows*. Con *Skype* possiamo sia eseguire chiamate tramite Internet, sia inviare e ricevere messaggi in tempo reale.

### 5.3.1. I rischi per la sicurezza sui sistemi di messaggistica istantanea

Come la posta elettronica, anche la messaggistica istantanea comporta notevoli rischi per la sicurezza delle nostre informazioni personali.

Proprio a causa della loro enorme diffusione, i servizi di messaggistica istantanea sono infatti diventati un bersaglio per gli hacker. Accedere a file personali, intercettare messaggi e conversazioni private sono infatti gli obiettivi privilegiati dagli hacker.

Le applicazioni di messaggistica istantanea possono dunque infettarsi e venire contagiate da malware. Il metodo con cui i malware si diffondono è sempre lo stesso: i file che ci scambiamo nelle chat possono contenere software infetto. Anche le GIF che tanto spesso

scambiamo insieme ai messaggi possono contenere software dannosi per la sicurezza delle nostre conversazioni private e dei nostri dati personali. Dobbiamo pertanto fare molta attenzione ai file che scambiamo e condividiamo nelle chat.

La soluzione più immediata che possiamo adottare per tutelare la nostra privacy è quella di *non* scambiare, durante le nostre conversazioni online, dati personali, immagini o foto, e di *non* aprire i link che ci vengono suggeriti, a maggior ragione se a suggerirceli sono persone a noi sconosciute.

### 5.3.2. La crittografia end-to-end (E2E)

Per rendere più sicure le nostre comunicazioni, quasi tutte le applicazioni di messaggistica istantanea utilizzano la crittografia end-to-end (E2E), la quale è in grado di difenderci dagli attacchi *Man In The Middle* (MITM). Con questi attacchi, gli hacker si inseriscono nelle comunicazioni tra due utenti (*in the middle*, appunto) per rubare le loro informazioni personali.

La crittografia end-to-end funziona così: ogni messaggio viene criptato appena inviato e decriptato quando viene ricevuto, tramite una chiave che possiede solo il destinatario. La criptazione e decriptazione dei dati avviene sia sul computer del mittente che sul computer del destinatario, e non su un server esterno.

Questo sistema di trasmissione dei dati è tra i più sicuri, ma ciò non implica che le nostre conversazioni siano al sicuro. C'è sempre il rischio che qualcuno possa riuscire a intercettarle e decifrarle.

La *Electronic Frontier Foundation* (EFF), un gruppo di pressione che ha lo scopo di difendere le libertà civili nel mondo digitale, ha fornito alcune importanti informazioni su come le aziende che gestiscono le varie applicazioni di messaggi curano la privacy dei loro utenti. Emerge che le applicazioni più usate al mondo hanno moltissime falle.

Secondo il rapporto della EEF un'app di messaggi veramente sicura dovrebbe avere i seguenti requisiti:

- Criptare i messaggi in tutte le fasi della comunicazione. Usando la crittografia E2E, anche i dipendenti dell'azienda non potrebbero accedervi

- Possibilità di verificare istantaneamente l'interlocutore.
- Sicurezza della cronologia delle comunicazioni nel caso in cui le chiavi di crittografia venissero rubate
- Il codice della app può essere giudicato da ispettori esterni e indipendenti
- La progettazione e la realizzazione della crittografia deve essere documentata
- Il codice è stato controllato nel corso dell'ultimo anno

Preso atto di tutto ciò, elenchiamo alcune applicazioni di messaggistica istantanea che rispettano i parametri proposti da EEF:

- *ChatSecure*, per *Android* e *iOS*, è gratis e utilizza librerie open source crittografiche, come XMPP, OTR e Tor, per garantire che i messaggi rimangano completamente privati.
- *Silent Circle* è un'applicazione a pagamento per *Android* e *iOS* che funziona un po' come *Skype* e permette di fare telefonate e videochiamate completamente criptate. È anche possibile chiamare utenti che non hanno l'applicazione installa; la chiamata sarà ugualmente crittografata.
- *Signal Messenger* è la chat cifrata per *Android* e *iOS*, con cui fare telefonate protette da intercettazioni. È possibile anche inviare messaggi istantanei con testo, immagini e video nelle chat.
- *Telegram* non ha un punteggio perfetto, ma rimane comunque un'app di messaggistica sicura quasi al 100%.
- *Wickr* è un'app per *Android* e *iOS* con crittografia end-to-end. La particolarità di questa applicazione speciale, molto usata dagli hacker, è che è una chat con messaggi che si autodistruggono.

## 5.4. Dispositivi mobili

Smartphone e tablet sono i dispositivi mobili più diffusi. Le prestazioni di questi dispositivi sono con il tempo migliorate, tanto da consentirci di compiere operazioni che fino a qualche tempo fa avremmo potuto concludere soltanto con i computer.

I dispositivi mobili si distinguono in base al loro sistema operativo, ossia il software principale che ne consente il funzionamento. In commercio, troviamo i dispositivi mobili che utilizzano il sistema operativo *Android*, e i dispositivi mobili della *Apple* che invece utilizzano il sistema operativo *iOS*.

Come ogni altro computer, anche i dispositivi mobili possono infettarsi. Gli hacker infatti progettano malware specifici con cui attaccare i dispositivi mobili. Dobbiamo pertanto fare attenzione quando li utilizziamo, ed evitare che possano trasformarsi in strumenti dannosi.

### 5.4.1. Cosa sono le autorizzazioni

Le applicazioni per dispositivi mobili (le così dette *app*) vanno scaricate dagli *app store*, negozi virtuali nei quali possiamo trovare ogni tipo di app, sia a pagamento che gratuite.

Ogni sistema operativo utilizza un app store ufficiale. L'app store del sistema operativo *Android* si chiama *Play Store*, mentre quello del sistema operativo *iOS* si chiama *Apple app store*. Gli app store sono già installati sui nostri dispositivi mobili, pertanto non dobbiamo eseguire alcuna operazione per disporne.

Subito prima di avviare il procedimento per installare l'app che abbiamo scaricato dall'app store, il sistema operativo ci mostra l'elenco con le autorizzazioni che dobbiamo fornire per far sì che l'app possa funzionare correttamente.

Le autorizzazioni ci fanno capire i dati a cui l'app potrà accedere una volta completata la sua procedura di installazione. Sono dunque dei permessi che forniamo all'app, in modo che possa funzionare correttamente.

Un'app per scattare foto o registrare video, ad esempio, avrà bisogno del nostro permesso prima di utilizzare la fotocamera del dispositivo su cui la installeremo. Le app per utilizzare i social network invece ci chiedono le autorizzazioni per accedere alla lista dei nostri contatti, in modo da avere un gruppo di persone con cui possiamo iniziare a comunicare. Un'app di navigazione satellitare, per fare un altro esempio, ci chiederà di accedere alla nostra posizione, in modo da sapere dove ci troviamo prima di fornirci le indicazioni che cerchiamo.

Alcune app invece possono chiederci le autorizzazioni per accedere ai nostri dati personali, come conversazioni, messaggi privati, foto, e molto altro. Queste richieste vengono visualizzate la prima volta che l'app deve accedere ai nostri dati.

Le app potenzialmente dannose invece chiedono autorizzazioni che non sono indispensabili per il loro funzionamento. Se ad esempio un gioco ci chiede l'autorizzazione per accedere alla nostra fotocamera, possiamo stare ben certi che molto probabilmente si tratta di un malware.

Le autorizzazioni più pericolose, cioè quelle a cui prestare maggiore attenzione, includono l'accesso alla cronologia delle chiamate, ai messaggi privati, alla posizione, alla fotocamera e al microfono. Per alcune app, queste autorizzazioni sono necessarie, per altre non lo sono. In ogni caso, è sempre meglio controllare che l'app sia sicura prima di installarla, e accertarsi che provenga da un fonte affidabile.

### 5.4.2. Controllare le autorizzazioni richieste delle app

In molti casi, nessuno di noi controlla le autorizzazioni richieste dalle app. Praticamente tutti acconsentiamo ai permessi che le app ci chiedono di fornire prima della loro installazione, senza neanche controllare i dati a cui potranno accedere.

Proprio per questo motivo, possiamo controllare le autorizzazioni che abbiamo concesso anche dopo aver installato una app. Nel sistema operativo *Android*, procedi come segue:

1. Apri l'app *Impostazioni*, quindi fai tap su *Applicazioni*.
2. Fai tap sul nome dell'app di cui desideri controllare le autorizzazioni.
3. Nella sezione *Privacy*, fai tap su *Autorizzazioni*.
4. Controlla le autorizzazioni da te concesse quando hai installato l'app sul tuo dispositivo.
5. Se noti qualcosa di strano, come ad esempio un'autorizzazione inappropriata, rimuovi l'app.

Nei dispositivi mobili della *Apple* sui quali è installato il sistema operativo *iOS*, per controllare in che modo le app utilizzano i permessi che hai concesso, devi seguire questi passaggi:

1. Apri l'app *Impostazioni*, quindi fai tap su *Privacy*.
2. Fai tap su *Resoconto sulla privacy delle app*.

Il resoconto sulla privacy delle app mostra in che modo le app utilizzano i permessi da te concessi, e mostra la loro attività di rete.

**Attenzione**. Fai attenzione alle app che chiedono l'accesso ai sensori del tuo dispositivo, come la fotocamera e il microfono; alle app che ti chiedono di accedere ai messaggi, contatti e calendari; alle app che ti chiedono di accedere alle chiamate; e infine alle app che ti chiedono di conoscere la tua posizione GPS. Per alcune app, queste autorizzazioni sono necessarie. In questi casi, prima di installare l'app, verifica che sia sicura, e che provenga da una fonte affidabile.

### 5.4.3. Cosa fare se perdiamo il nostro dispositivo

Ci sono azioni specifiche che possiamo compiere nel caso in cui smarrissimo il nostro dispositivo mobile. La prima di queste azioni è localizzare il dispositivo. Possiamo in questo modo conoscere la sua posizione, e provare a rintracciarlo. Per evitare che altre persone possano accedervi e conoscere le nostre informazioni personali, possiamo bloccare il dispositivo, ed eventualmente cancellare tutti i contenuti nella sua memoria (in questo caso, non potremo più localizzare il dispositivo). Tutte queste operazioni vanno eseguite da un computer o da un altro dispositivo mobile.

**Attenzione.** Per localizzare, bloccare o resettare il dispositivo smarrito, occorre che il dispositivo sia acceso; che sia associato a un account *Google* (nel caso dei dispositivi con il sistema operativo *Android*), o a un *ID Apple* (nel caso degli *iPhone* o *iPad*); che sia connesso a una rete di dati mobile o Wi-Fi; e che sia attiva la funzione per la localizzazione del dispositivo.

Nel caso in cui smarrissi il tuo dispositivo *Android*, collegati alla pagina web *google.com/android/find*, ed esegui il login per accedere al tuo account *Google*.

Nella finestra del tuo browser, verrà aperta la scheda *Trova il mio dispositivo*, al cui interno visualizzi la mappa con la posizione del dispositivo.

A questo punto, puoi decidere di compiere una delle seguenti operazioni:

- Fare squillare il dispositivo per cinque minuti, in modo da verificare se si trova nelle tue vicinanze.
- Bloccare il dispositivo e uscire dal tuo account *Google*. In questo caso, puoi lasciare un messaggio o un numero di telefono a cui farti contattare da chiunque trovi il tuo dispositivo.
- Resettare il dispositivo. In questo caso, tutti i contenuti del dispositivo verranno cancellati, e non potrai più localizzarlo.

**Suggerimento**. Per localizzare il dispositivo smarrito, puoi anche utilizzare l'app gratuita *Trova dispositivo.* Se questa app non è tra quelle già installate sul dispositivo che utilizzi per localizzare il dispositivo smarrito, collegati al *Play store* per scaricarla.

**Nota**. Ogni dispositivo di telefonia mobile (cellulari, smartphone, tablet, ecc.) ha un codice di quindici cifre che lo identifica. Si tratta del codice IMEI, associato al dispositivo dal suo produttore. Il codice IMEI non va confuso con la SIM. Il codice IMEI infatti identifica il dispositivo al quale viene associato, mentre la SIM identifica l'intestatario del contratto sottoscritto con un gestore di telefonia mobile. Nel caso in cui smarrissimo o perdessimo il nostro dispositivo, possiamo fornirne il codice IMEI al nostro gestore telefonico, e chiederne il blocco. In questo modo, impediremo a malintenzionati di accedere alle nostre informazioni personali. Il codice IMEI è riportato sulla confezione del dispositivo, altrimenti possiamo digitare la combinazione *#06# sulla tastiera del dispositivo per accedere alla scheda con il codice IMEI. Il codice IMEI può essere utilizzato per localizzare il dispositivo smarrito o rubato. Dopo la denuncia, le autorità competenti possono infatti utilizzare il codice IMEI per risalire all'ultima posizione del dispositivo, e tentare dunque di recuperarlo.

# 6. Mettere al sicuro i propri dati

## 6.1. Il backup dei dati

Siamo tutti oramai abituati a creare continuamente file. Quando scattiamo una foto con il nostro smartphone, ad esempio, creiamo un file che viene automaticamente archiviato nella memoria del nostro dispositivo. La stessa cosa accade quando registriamo un video o scarichiamo un file da Internet. Anche i numeri di telefono che memorizziamo sul nostro smartphone sono file che vengono aggiunti alla lista dei contatti.

I nostri computer inoltre possono contenere file per noi molto importanti, come documenti di lavoro o di studio, informazioni personali di ogni tipo, cronologia dei siti Internet, lista dei preferiti, foto, video, file musicali, ecc.

Come possiamo recuperare i dati che abbiamo perso in seguito al furto o allo smarrimento del nostro dispositivo, o in seguito a un guasto del nostro computer?

Per evitare problemi di questo genere, è buona norma creare copie di sicurezza dei propri dati, che nel gergo informatico vengono definite *copie di backup*.

### 6.1.1. Creare copie di backup dei dati su un supporto esterno

Come abbiamo già detto, è buona norma creare sistematicamente copie di sicurezza dei propri dati, almeno di quelli più importanti. Il modo più semplice per fare ciò è duplicarli su un supporto esterno, come un disco rimovibile, un hard disc, una chiave usb o una scheda di memoria SD. Vediamo dunque come creare copie di backup dei dati nel sistema operativo *Windows 11*.

1. Collega al tuo computer il supporto esterno sul quale desideri realizzare la copia di backup dei tuoi dati. Se utilizzi un supporto usb, collegalo a una porta usb del tuo computer. Di solito tutti i computer, sia desktop che laptop, dispongono di una o più porte usb.
2. Nella barra delle applicazioni di *Windows 11*, seleziona il pulsante *Esplora file*. L'icona di questo pulsante è una cartella marrone chiaro  .

3. Ci sono due tipi di cartelle: quelle che tu o un altro utente avete creato, e che pertanto puoi modificare, spostare e rinominare a tuo piacimento, e quelle che invece sono parte di *Windows 11*, e si chiamano pertanto *cartelle di sistema*. Ad esempio, le cartelle *Documenti* e *Download* sono cartelle di sistema. Puoi usare le cartelle di sistema per salvare file, ma non puoi modificarle, rinominarle o eliminarle.

4. Raggiungi la cartella con i file di cui desideri eseguire una copia di backup.

5. Fai clic sulla cartella, in modo da accedere ai file al suo interno.

6. Seleziona i file di cui desideri eseguire il backup, e nella barra superiore della finestra di dialogo *Esplora file*, fai clic sul pulsante *Copia*. Questa operazione crea una copia temporanea dei file selezionati, che viene posizionata in uno specifico spazio di *Windows 11*, chiamato *Appunti* (*Clipboard* in americano).

7. Nel menu a sinistra della finestra di dialogo *Esplora file*, fai clic sull'icona del supporto esterno collegato al computer, nel quale intendi duplicare i file copiati (nella Figura 6.1, il supporto esterno collegato al computer si chiama semplicemente "USB"). Se i file nel supporto esterno sono già organizzati in una o più cartelle, a sinistra dell'icona, compare una piccola freccia verso destra. Cliccando su questa piccola freccia, puoi accedere alle cartelle racchiuse del supporto esterno.

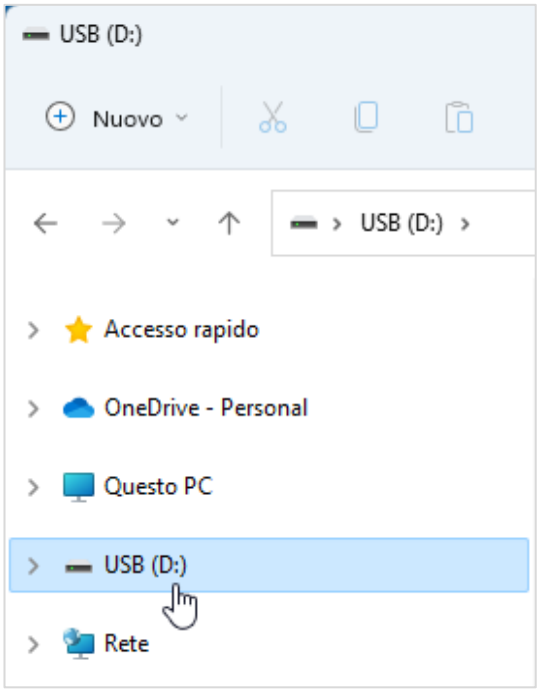



*Figura 6.1 — Accedere dal sistema operativo Windows 11 a un supporto esterno collegato al computer*

8. Raggiungi la posizione in cui desideri salvare la copia di backup dei dati.

9. Nella barra superiore della finestra di dialogo *Esplora file*, fai clic sul pulsante *Incolla*  .

**Nota**. In alcuni casi, prima di utilizzare hard disk esterni, chiavi usb, schede SD, è necessario eliminare tutti i file e cartelle al loro interno, in modo da fare spazio per accogliere le copie di backup dei dati. La *formattazione* ci permette di eliminare in fretta e con un'unica operazione tutti i dati contenuti in un'unità di qualsiasi tipo (hard disc esterni, chiavi usb, schede SD). In *Windows 11*, (1) inserisci nell'apposita porta del computer il supporto esterno da formattare; (2) nella barra delle applicazioni, fai clic sul pulsante *Esplora file*; (3) nel menu a sinistra della finestra di dialogo che si apre, fai clic con il tasto destro del mouse sull'icona del supporto da formattare; (4) nel menu contestuale che compare, seleziona l'opzione *Formatta*; (5) nella finestra di dialogo che si apre, seleziona *Avvia*. Con la formattazione, ogni file nel supporto esterno viene eliminato.

### 6.1.2. Archiviare file su OneDrive

L'installazione di *Windows 11* dà anche diritto all'uso gratuito di *OneDrive* con uno spazio di archiviazione di 5 GB. *OneDrive* infatti è il nome del servizio di archiviazione sul cloud, che la *Microsoft* mette a disposizione di ogni utente di *Windows*.

Possiamo raggiungere *OneDrive* dalla finestra di dialogo *Esplora file* di *Windows 11*. Per aprirla, è sufficiente fare clic sull'icona a forma di cartella sulla barra delle applicazioni di *Windows* 11.

*OneDrive* è anche il nome della cartella predisposta nel computer, nella quale possiamo inserire intere cartelle e singoli file, affinché vengano integralmente trasferiti nel nostro spazio di archiviazione online.

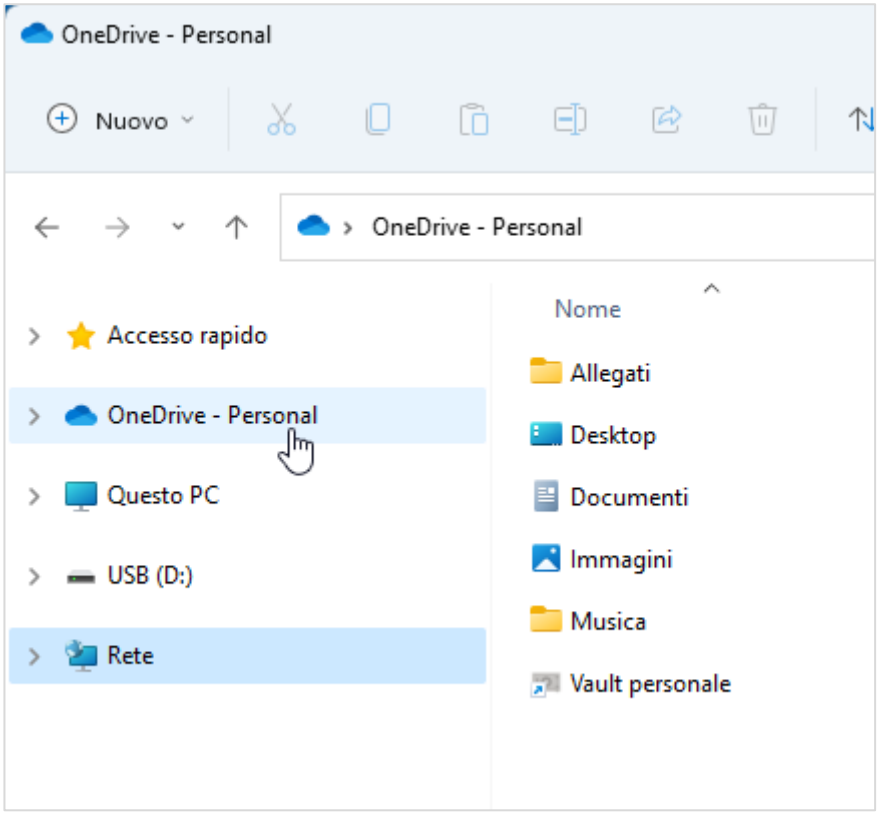



*Figura 6.2 — La cartella OneDrive nella finestra di dialogo Esplora file*

Il modo più semplice per inserire file e cartelle in *Onedrive* è per trascinamento. Una volta raggiunti gli elementi che vogliamo inserire, è sufficiente farci clic sopra e tenere premuto il pulsante sinistro del mouse, mentre li spostiamo nella cartella *OneDrive*.

In alternativa, possiamo copiare gli elementi da inserire nel nostro spazio di archiviazione online, e poi incollarli nella cartella *OneDrive* del computer.

La cartella *OneDrive* è collegata con il nostro account *Microsoft*. Ciò significa che possiamo utilizzare qualsiasi computer o dispositivo per accedere ai suoi contenuti, l'importante è aver prima eseguito il login per accedere al nostro account *Microsoft*.

Gli elementi che aggiungiamo nella cartella *OneDrive*, inoltre, vengono automaticamente sincronizzati con ogni altro computer o dispositivo, in cui la cartella *OneDrive* è associata al medesimo account *Microsoft*.

Per inserire file su *OneDrive*, occorre che il computer resti collegato a Internet per tutta la durata del loro caricamento. Se tuttavia il collegamento a Internet dovesse interrompersi,

la sincronizzazione dei file su *OneDrive* verrà automaticamente completata non appena il computer si riconnette a Internet.

Nel nostro spazio di archiviazione su *OneDrive*, ci sono diverse cartelle predefinite, ossia *Allegati*, *Desktop*, *Documenti*, *Immagini*, *Musica* (vedi la Figura 6.2). Come vedremo nel paragrafo successivo, le cartelle predefinite *Desktop*, *Documenti* e *Immagini* possono essere impiegate per archiviare copie di sicurezza dei file più importanti.

Una volta che inseriamo elementi nella cartella *OneDrive* del nostro computer, nella colonna *Stato* della finestra di dialogo *Esplora file*, possono comparire due tipi di icone:

- La nuvoletta indica che il file è disponibile soltanto online. Ciò significa che non occupa spazio sul disco fisso del nostro computer. Grazie alla sincronizzazione, il file è inoltre accessibile da qualsiasi altro dispositivo.
- Il cerchietto con un segno di spunta verde al suo interno indica che il file è disponibile sia online sia localmente.

Per aprire un file che si trova su *OneDrive*, in modo da poterci continuare a lavorare, è sufficiente aprire la finestra di dialogo *Esplora file*, accedere alla cartella *OneDrive*, e infine fare doppio clic sull'icona del file. Il file viene prima scaricato localmente, e poi aperto con l'applicazione che è in grado di gestirlo.

**Nota**. Come abbiamo già detto, l'installazione di *Windows 11* dà diritto all'uso gratuito di *One Drive* con uno spazio di archiviazione di 5 GB. Sottoscrivendo un piano a pagamento, tuttavia, è possibile usufruire di uno spazio di archiviazione maggiore. Nel momento in cui scriviamo, il piano *Microsoft 365 Family* permette di scaricare le applicazioni di *Office*, e di usufruire di uno spazio di archiviazione nel cloud di 6 terabyte (ovvero 1 terabyte a persona).

### 6.1.3. Eseguire copie di backup dei dati su OneDrive

*OneDrive* è utile anche per eseguire il backup dei nostri file più importanti. Per usufruire di questa funzione, dobbiamo però ricordarci di memorizzare questi file all'interno di specifiche cartelle di *Windows 11*. In pratica, possiamo configurare *OneDrive*, affinché i file nelle cartelle *Desktop*, *Documenti* e *Immagini* di *Windows 11* vengano automaticamente copiati nel nostro spazio di archiviazione sul cloud della *Microsoft*.

Per configurare il backup dei file più importanti su *OneDrive*, segui questi passaggi:

1. Nella barra delle applicazioni di *Windows 11*, seleziona il pulsante *Start*, quindi fai clic su *Impostazioni*.
2. Nel menu a sinistra della finestra *Impostazioni*, seleziona *Account* > *Backup di Windows*.
3. Seleziona il pulsante *Gestisci le impostazioni di sincronizzazione*.
4. Nella finestra di dialogo che si apre, fai clic su *Avvia Backup*.

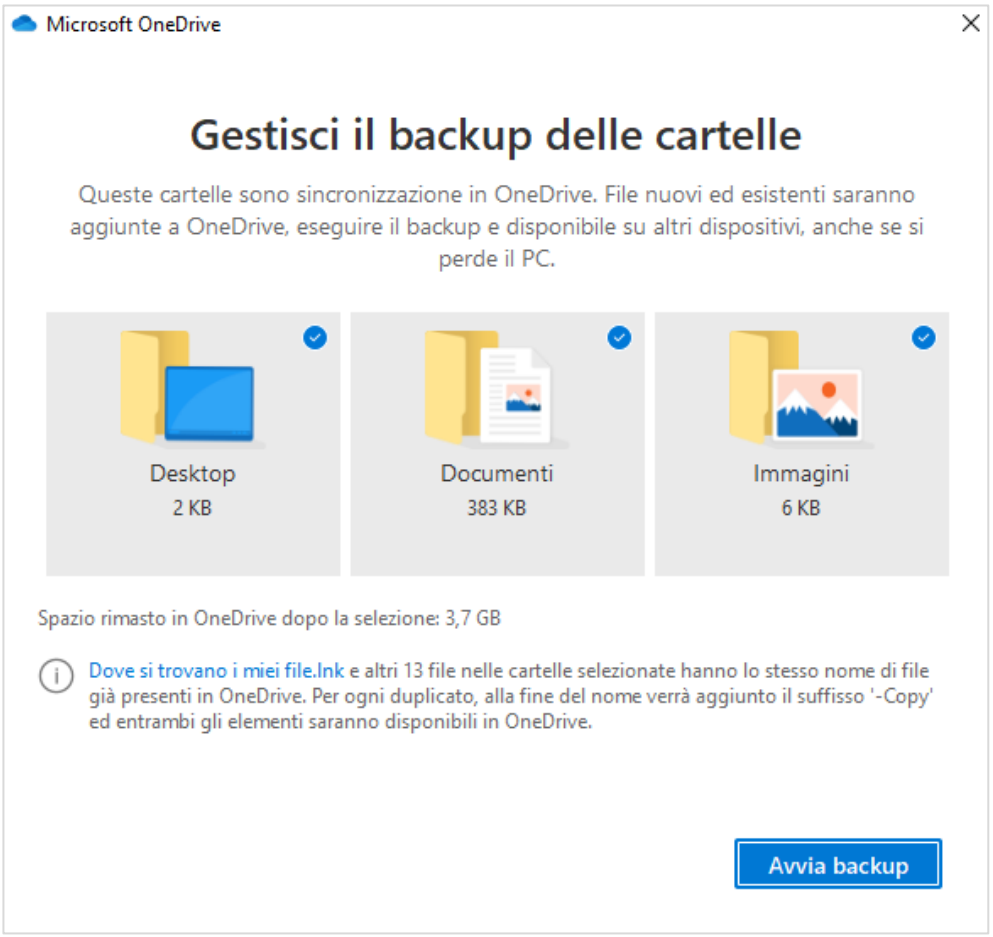



*Figura 6.3 — Eseguire il backup delle cartelle Desktop, Documenti e Immagini in Onedrive*

**Nota**. Al termine del backup, le cartelle *Desktop*, *Documenti* e *Immagini* del tuo computer vengono sincronizzate con le stesse cartelle su *OneDrive*. Questa configurazione inoltre ti permette di realizzare automaticamente copie di backup su *OneDrive* anche dei nuovi file che man mano aggiungi nelle cartelle *Desktop*, *Documenti* e *Immagini* del tuo computer.

Per interrompere il backup dei dati su *OneDrive*, fai clic sul pulsante *Start*, quindi seleziona *Impostazioni* > *Account* > *Backup di Windows* > *Gestisci le impostazioni di sincronizzazione*. Per interrompere il backup di una cartella, seleziona *Interrompere Backup*, dopodiché conferma la tua scelta.

**Attenzione**. Quando interrompi il backup di una cartella, i file di cui hai già eseguito il backup restano su *OneDrive*, ma non vengono più visualizzati nella cartella del tuo computer. Se ad esempio hai interrotto il collegamento della cartella *Desktop* del tuo computer con *OneDrive*, sul tuo computer non potrai più visualizzare i file di cui hai eseguito il backup, ma ciò non significa che siano stati cancellati dal tuo computer. Nella cartella di cui hai interrotto il backup comparirà un'icona chiamata *Dove sono i miei file*. Questa icona in realtà è un collegamento: cliccando su di essa, infatti, puoi accedere direttamente alle tue cartelle su *OneDrive*, e scaricare manualmente i file sul tuo dispositivo.

### 6.1.4. Pianificare il backup dei dati su un supporto esterno

Il sistema operativo *Windows* include una specifica funzione con cui pianificare il backup dei dati.

1. Collega al tuo computer il supporto esterno sul quale desideri realizzare una copia di backup dei dati.
2. Nella barra delle applicazioni di *Windows 11*, seleziona la lente di ingrandimento.
3. Nella casella superiore del pannello che si apre, digita il testo "Pannello di controllo", quindi fai clic su *Apri*.
4. Nella sezione *Sistema e sicurezza*, fai clic sull'opzione *Backup e ripristino*.
5. Fai clic su *Configura backup*.
6. Nella finestra di dialogo che si apre, seleziona il supporto esterno in cui salvare la copia di backup dei dati, quindi fai clic su *Avanti*.
7. Assicurati che ci sia il segno di spunta nella casella *Seleziona automatica*. In questo modo, eseguirai il backup dei dati archiviati nei cataloghi, nel desktop e nelle cartelle predefinite di *Windows*.
8. Fai clic su *Avanti*, quindi verifica le impostazioni del backup.

9. Per specificare la frequenza con cui eseguire il backup dei dati, fai clic su *Modifica pianificazione*.

10. Nella finestra di dialogo che si apre, inserisci la frequenza, il giorno e l'orario in cui eseguire automaticamente il backup, e poi fai clic su *OK*.

11. Se la configurazione del backup soddisfa le tue esigenze, fai clic su *Salva impostazioni ed esegui backup*.

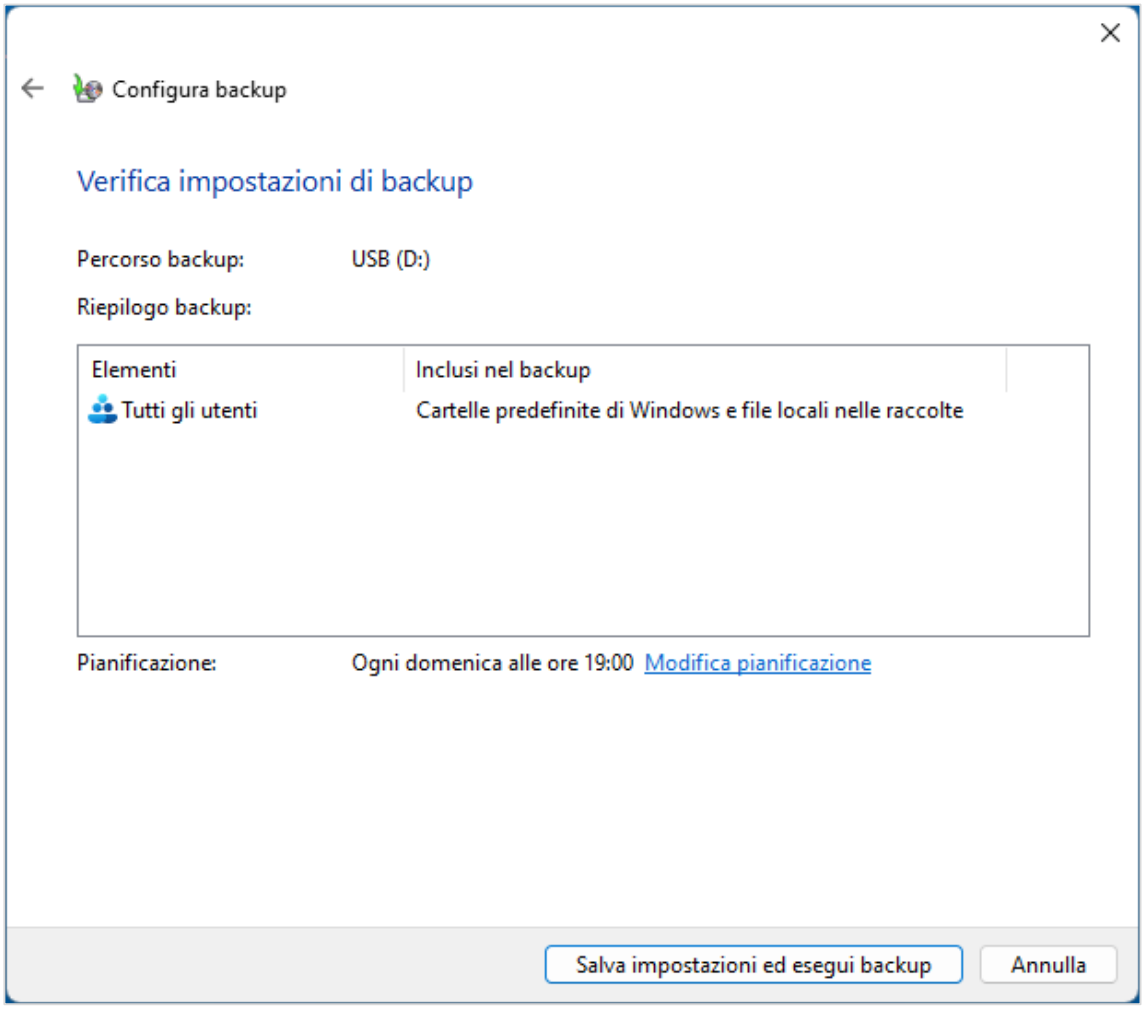



*Figura 6.4 — Configurare e pianificare il backup dei dati con il sistema operativo Windows*

**Attenzione**. La procedura per concludere il backup può richiedere molto tempo. Durante il backup, il computer deve rimanere acceso e collegato al supporto esterno sul quale salvare il file di backup.

Per disattivare la pianificazione del backup, segui la procedura che abbiamo visto poco fa fino al punto 4, e nella sezione in alto a sinistra della finestra di dialogo *Backup e ripristino*, seleziona l'opzione *Disattiva pianificazione*.

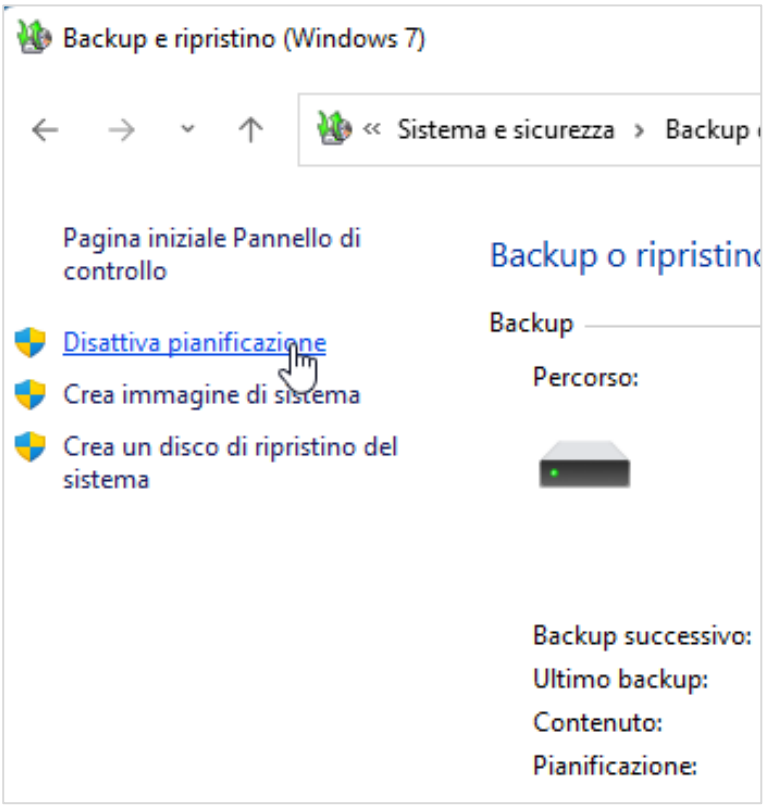



*Figura 6.5 — Disattivare la pianificazione del backup dei dati*

### 6.1.5. Ripristinare dati da una copia di backup

Nel caso in cui i dati siano andati persi o siano stati danneggiati, possiamo procedere al loro recupero. In gergo informatico, la procedura per recuperare i dati persi o danneggiati si chiama *ripristino*.

Il modo più semplice che possiamo seguire per ripristinare i dati persi o danneggiati è quello di collegare al nostro computer il supporto esterno sul quale abbiamo salvato la copia di backup dei dati, per poi individuare manualmente i file e le cartelle da ripristinare. Una volta copiati, possiamo incollare questi elementi nella posizione del nostro computer in cui desideriamo ripristinarli.

Diversamente, possiamo decidere i file e le cartelle da ripristinare. In questo caso, procedi come segue:

1. Collega al tuo computer il supporto esterno dal quale recuperare la copia di backup dei dati.
2. Nella barra delle applicazioni di *Windows 11*, seleziona la lente di ingrandimento.
3. Nella casella superiore del pannello che si apre, digita il testo "Pannello di controllo", quindi fai clic su *Apri*.
4. Nella sezione *Sistema e sicurezza*, fai clic sull'opzione *Backup e ripristino*.
5. Seleziona il pulsante *Ripristina i file personali*.
6. Nella finestra di dialogo *Ripristina file*, puoi scegliere i file da ripristinare.
    - Per cercare nel backup i singoli file da ripristinare, fai clic su *Cerca file*, quindi raggiungi e seleziona i file. Fai clic su *Aggiungi file*, per predisporre il ripristino dei file selezionati.
    - Per cercare nel backup le singole cartelle da ripristinare, fai clic su *Cerca cartelle*, quindi raggiungi e seleziona le cartelle. Fai clic su *Aggiungi cartella*, per predisporre il ripristino delle cartelle selezionate.
7. Fai clic su *Avanti*.

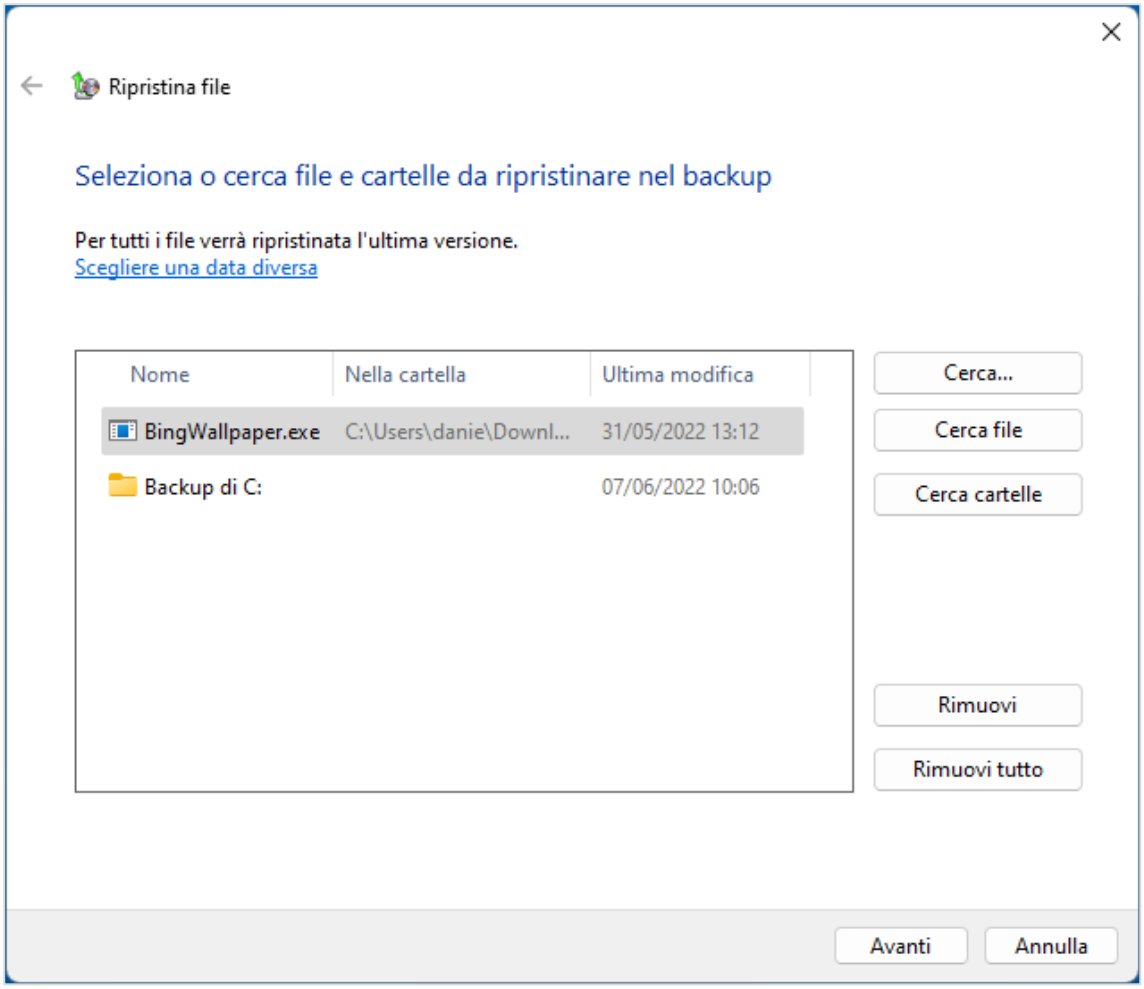



*Figura 6.6 — La finestra di dialogo di Windows da cui scegliere i file e cartelle da ripristinare*

8. Scegli in quale cartella ripristinare i file. Puoi ripristinarli nel loro percorso originale, oppure indicarne un altro.

9. Fai clic su *Ripristina*.

**Attenzione**. La procedura di ripristino può richiedere molto tempo. Durante il ripristino dei dati, il computer deve rimanere acceso e collegato al supporto esterno sul quale salvare il file di backup.

## 6.2. Eliminare i dati

I file che non ci servono più, è buona norma cancellarli. Se ci abituiamo a compiere frequentemente questa operazione, potremo risparmiare molto spazio sul nostro computer o dispositivo mobile.

### 6.2.1. Eliminare i dati dal computer e dai supporti esterni

Il *Cestino* è la cartella di *Windows* nella quale vengono spostati i file una volta eliminati. Non è possibile in alcun modo eliminare, modificare o rinominare questa cartella.

Dopo averli spostati nel *Cestino*, i file scompariranno a tutti gli effetti dalla loro posizione iniziale, ma ciò non significa che verranno eliminati definitivamente dal computer. È infatti possibile ripristinare i file eliminati, anche dopo averli spostati nel *Cestino*.

Anche quando svuotiamo il *Cestino*, il sistema operativo non elimina del tutto i dati al suo interno, ma etichetta lo spazio da loro occupato sul disco rigido come utilizzabile. Ciò significa che il sistema operativo utilizzerà questo spazio per aggiungere nuovi dati. Fin quando i nuovi dati non saranno abbastanza capienti da sovrascrivere completamente quelli che sono stati eliminati, sarà sempre possibile recuperare questi dati, anche soltanto per la parte che ancora non è stata sovrascritta.

Utilizzando specifici software è infatti possibile trovare nel computer le tracce dei file rimossi, e ricostruirli integralmente o quasi. La capacità di questi software di riuscire a riscostruire i file una volta eliminati dal *Cestino* dipende da quanto tempo è passato dalla loro cancellazione, e dai successivi utilizzi del computer.

Anche quando formattiamo un disco rigido, una chiave usb, una scheda SD, o un qualsiasi altro supporto di memoria, in realtà non stiamo eliminando i dati in modo permanente. I dati sono sempre recuperabili, soprattutto se ricorriamo alla formattazione rapida per resettare un disco rigido o un supporto di memoria. La formattazione rapida infatti identifica i dati come sovrascrivibili, senza eliminarli del tutto. In questo modo, i nuovi dati sovrascrivono quelli che già c'erano.

### 6.2.2. Eliminare definitivamente i dati

Il modo più sicuro per eliminare definitivamente i dati dal proprio computer è quello di distruggere il disco rigido o il supporto di memoria che li contiene. Soltanto in questo modo, potremo essere sicuri di aver cancellato in modo irreversibile i dati, e di aver fatto scomparire ogni loro traccia.

Esistono tuttavia delle alternative meno cruente e invasive che assicurano una cancellazione sicura dei dati.

*Glary Utilities*, oltre a recuperare i dati cancellati, può distruggerli in modo definitivo. Il metodo usato per eliminare definitivamente i dati è l'*American Dod 5220.22-M*, sviluppato dal Dipartimento della Difesa degli Stati Uniti d'America per rimuovere i dati di sicurezza.

*CCleaner* è un altro software con cui possiamo cancellare dal nostro computer tutti i file che non sono più utili. Questo programma è in grado di cancellare anche tutti i file che registrano le tracce della nostra navigazione in Internet, e che vengono automaticamente salvati sul nostro computer. Questo tipo di pulizia ha innegabili vantaggi. Per prima cosa, libera lo spazio sul disco rigido del computer; difende inoltre la nostra privacy; e infine rende più veloce il sistema operativo.