EUROPEAN INFORMATICS PASSPORT

SICUREZZA INFORMATICA

Dispensa di approfondimento

European e-Competence Framework

ACCREDITATO DAL MIUR PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA - DIRETTIVA 170/2016 E IN LINEA CON L'E-CF E IL DIGCOMP2.1

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.

Segni convenzionali

Utilizziamo tre icone per sottolineare informazioni rilevanti, su cui ti consigliamo di soffermarti.

Suggerimenti. Questa icona contrassegna spunti e scorciatoie utili per risparmiare tempo o gestire con più facilità una determinata operazione.

Attenzione. Aguzza la vista quando vedi questa icona: ti stiamo dando indicazioni utili per gestire i passaggi più complicati o rilevanti per il tuo percorso.

Nota. Non trascurare gli approfondimenti e le curiosità contrassegnate con questa icona; potrebbero esserti utili per comprendere a fondo l'argomento trattato.

Certipass
Centro Studi

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.

Indice

1. DEFINIZIONI

L'IT Security rappresenta l'insieme delle tecnologie e dei processi progettati per garantire la protezione di reti, sistemi operativi, programmi, dati e informazioni da accessi non autorizzati, attacchi e danni.

In ambito informatico, i *dati* sono numeri, lettere, immagini, suoni, simboli ecc., ai quali viene attribuito un significato, affinché rappresentino una realtà, in maniera elementare.

Più dati, elaborati e associati ad altri fattori attraverso un computer, danno vita a un'*informazione*.

Più precisamente, l'informazione è il risultato dell'interpretazione di un insieme di dati che possono incrementare le conoscenze di un soggetto. Il termine deriva dal latino e significa *dare forma alla mente*, ossia insegnare.

1.1 Le finalità dell'IT Security

Lo scopo principale dell'IT Security è quindi garantire la protezione dell'integrità fisica (*hardware*) e logico-funzionale (*software*) di un sistema informatico e dei dati in esso contenuti o scambiati in rete, minimizzandone la vulnerabilità.

Differenti tipi di insidie minacciano:

- il funzionamento delle applicazioni,
- la riservatezza delle informazioni immagazzinate sui computer e veicolate attraverso Internet.

È un tema centrale, considerata la pervasività dell'ICT nella sfera privata e lavorativa di tutti noi.

Più tecnologia usi per svolgere le tue attività quotidiane, più cresce il rischio di perdere o subire un furto di dati e informazioni.

1.1.1 Gli standard di sicurezza informatica

Gli standard di sicurezza informatica definiscono le regole che le organizzazioni devono attivare 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 impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese *Information Security Management System*), e include aspetti relativi alla sicurezza logica, fisica e organizzativa.

La versione più recente della norma è la ISO/IEC 27001:2013, che andrà gradualmente a sostituire la versione 2005.

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

1.1.2 Cosa proteggere?

Nell'ambito dell'IT Security, quindi, si protegge:

- l'insieme delle componenti essenziali del computer (sistemi operativi, programmi e dati),
- le reti che mettono in connessione i singoli dispositivi informatici.

Per comprendere a pieno le implicazioni di questo argomento, è indispensabile soffermarsi sulla definizione teorica di sicurezza informatica.

Il rischio, in genere, è la risultante dell'equazione tra minaccia/vulnerabilità e contromisure.

- La *minaccia* rappresenta l'azione capace di nuocere.
- La *vulnerabilità* rappresenta il livello di esposizione rispetto alla minaccia in un determinato contesto.
- La *contromisura* è l'insieme delle azioni attuate per prevenire la minaccia.

Ci preme sottolineare che le contromisure non sono unicamente soluzioni tecniche ma anche il risultato della formazione e della sensibilizzazione rivolte agli utenti. Per poter rendere sicuro un sistema, è necessario identificare le minacce potenziali per conoscere e prevedere le possibili strategie del male intenzionato.

Obiettivi della sicurezza informatica

La sicurezza informatica, in generale, consiste nell'assicurare che le risorse hardware e software di un'organizzazione o di un utente siano usate unicamente nei casi e nei modi previsti dalle norme e dagli accordi intercorsi tra le parti.

L'obiettivo della sicurezza informatica è di garantire cinque aspetti dell'ICT:

- l'*integrità dei dati*: devono effettivamente essere quelli che le parti in causa legittimamente sono convinti che siano;
- la *confidenzialità*: solo le persone autorizzate devono poter accedere alle risorse scambiate;
- la *disponibilità*: coloro che ne hanno diritto devono poter sempre accedere a un servizio o alle proprie risorse;

- il *non ripudio*: una transazione o un'azione svolta non può essere negata a posteriori dall'operatore;
- l'*autenticazione*: assicura l'identità di un utente, garantendo a ciascun corrispondente che il suo partner sia effettivamente quello che crede.

1.1.3 I diversi tipi di minacce

Le minacce a cui sono esposti sistemi operativi, dati e informazioni sono riconducibili a due ordini di fenomeni.

- Gli *eventi accidentali*. Si tratta delle conseguenze di eventi non ponderabili e legati a elementi casuali quali, ad esempio, gli eventi atmosferici che determinano l'interruzione dell'erogazione di energia elettrica e possono avere delle conseguenze sui sistemi operativi e sui dati.
- Gli *eventi indesiderati*. Sono le operazioni compiute da soggetti intenzionati a danneggiare il funzionamento dei dispostivi o a sottrarre informazioni e dati. In questo caso possiamo distinguere ulteriormente tra:
  - attacchi *malevoli,* finalizzati a intaccare il funzionamento dei sistemi,
  - *accesso ai dispositivi da parte di soggetti non autorizzati* e finalizzati alla sottrazione di dati e informazioni.

1.1.4 Crimini informatici e hacker

Attacchi malevoli e accessi non autorizzati sono crimini informatici: sono, cioè, crimini caratterizzati dal fatto di essere stati compiuti attraverso l'utilizzo della tecnologia informatica.

Usando *dispositivi mobili di archiviazione e/o collegamenti remoti della rete*, un male intenzionato può compromettere, anche in maniera grave, il funzionamento di un PC (o di un altro dispositivo), minando l'integrità, la riservatezza e la disponibilità dei dati e delle informazioni immagazzinate.

Per la natura immateriale della minaccia, questo tipo di infrazioni sono più complesse da riconoscere e costituiscono, quindi, uno dei più importanti ambiti di studio dell'IT Security.

Chi è l'hacker

Avrai sicuramente già sentito la parola inglese *hacker*. Si utilizza per identificare gli autori di crimini informatici.

Come capita spesso, la traduzione non è proprio precisa, almeno rispetto alle origini. Quando negli USA si è cominciato a usarla (anni '50), questa parola aveva un'accezione positiva: indicava 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 utente 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 dell'espressione: il verbo *to hack* significa *tagliare, sfrondare, aprirsi un varco* fra le righe di codice che compongono un software).

Con l'andar del tempo, è emersa la figura dell'esperto informatico che, abusando delle proprie abilità, sfrutta eventuali buchi nel sistema informatico dell'organizzazione (o dell'utente) che ha preso di mira, per:

- mandare in crash il sistema stesso,
- sottrarre dati e informazioni da utilizzare a proprio piacimento.

Da qui è derivata la distinzione tra l'hacker *etico*, il programmatore, e l'hacker *immorale* che compie crimini informatici.

Il tema è articolato: comporta notevoli implicazioni, sociali e politiche. Si discute molto circa la liceità/moralità di azioni di hackeraggio messe in atto contro grandi organizzazioni, accusate dall'opinione pubblica di minare democrazia, libertà e benessere dei cittadini (banche, multinazionali, aziende che producono armi, case farmaceutiche e così via).

Categorie principali di criminali informatici

Aldilà delle riflessioni appena proposte, non ci sono dubbi circa l'illegalità di numerosi e specifici attacchi. Chi li identifica come coloro che sottraggono dati, li definisce, in maniera più precisa, *cracker*. Ci sono ulteriori categorie o suddivisioni:

- i *phracher* sono specializzati nel furto di programmi che offrono servizi telefonici gratuiti o nella penetrazione in computer e database di società telefoniche;
- i *phreaker* utilizzano numeri telefonici o carte telefoniche per accedere ad altri computer.

Generalizzando, si potrebbe dire che esistono due grandi categorie di *hacker*:

- i *black hat* delinquono,
- i *white hat* tengono alla loro moralità e alla legalità di tutte le azioni poste in essere.

1.1.5 I diversi livelli di protezione

Avendo compreso quali sono le minacce a cui sono esposti i nostri dispositivi, vediamo come difendersi. Distinguiamo, inizialmente, tra:

- *misure di protezione passive*, riconducibili ad accorgimenti fisico-materiali, quali, ad esempio, il posizionamento dei server (dei computer, cioè, che fungono da archivio per tutti i computer ad esso collegati) in luoghi sicuri, dotati di sorveglianza;
- *misure di protezione attive*, disponibili anche sul tu PC.

1.1.6 Esempi pratici di misure di protezione

Login e password

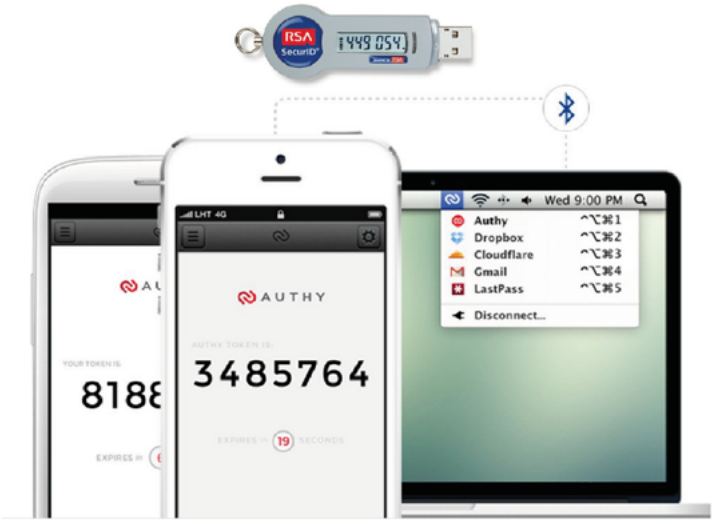
Per accedere a un PC e, poi, a qualsiasi account (di posta elettronica, di una home banking, di Facebook e così via), è necessario *autenticarsi*; è necessario, cioè, farsi riconoscere dal sistema, inserendo una password.

Senza password, non è possibile accedere al PC o a un qualsiasi account.

- Scegli le tue password utilizzando combinazioni non facili da indovinare: non usare mai i tuoi dati anagrafici!
- Abbiamo parlato al plurale: devi utilizzare password diverse per ognuno dei tuoi accessi (al PC, all'account di posta elettronica, a Skype e così via).
- È preferibile che siano composte da almeno 8 caratteri e siano composte da lettere maiuscole e minuscole, numeri e segni speciali (ad esempio, ! / ? _).

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 alla login: ogni volta che l'utente deve accedere al servizio, crea una password *usa e getta*.



1.1 | Generatori di OTP; sono sempre più usate apposite App per smartphone

Una volta che hai inserito correttamente *username* e *password* nella login (del tuo PC 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*.

L'autenticazione a due fattori

È uno dei metodi più sicuri per proteggere i tuoi account.

Il funzionamento è molto semplice: per poter accedere al tuo profilo Facebook o Twitter, oltre all'username e alla password, devi inserire il codice che ti viene spedito istantaneamente tramite SMS, e-mail o che puoi trovare su un'apposita applicazione.

Il metodo più usato è la ricezione di un SMS o di una e-mail contenente il PIN (un codice da 4 a 6 cifre) da inserire nella login per completare l'accesso al tuo profilo. Non è il più sicuro: un pirata informatico può hackerare il sistema e ricevere sul proprio smartphone il codice che hai richiesto tu.

Vediamo quali sono i metodi di autenticazione a due fattori più sicuri.

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.

Scansiona il codice QR; sullo schermo del tuo smartphone apparirà un nuovo PIN ogni trenta secondi; resterà valido e utilizzabile solo in questo brevissimo lasso di tempo; poi, ne vedrai un altro e così via. È sicuro perchè non c'è nessun intermediario tra l'utente e il server: nessun provider, nessun operatore telefonico. Molti servizi online consigliano l'utilizzo di un'applicazione per effettuare l'autenticazione a due fattori: Dropbox, Amazon, Google, Facebook e WhatsApp, solo per citarne alcuni.

Come sempre, nessuno strumento può difenderti se tu stesso non sei attento alle tue cose: a nulla varrebbe l'autenticazione appena vista se lasci il tuo smartphone incustodito o lo passi a chiunque.

One Button Authentication

È uno degli ultimi metodi realizzati per aumentare la sicurezza su Internet; viene, però, supportato da pochissime piattaforma 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.

Come la biometrica migliora la sicurezza informatica

Sai già che sugli smartphone più recenti ci sono lettori per le impronte digitali e altri sensori biometrici. A cosa servono?

Servono a rafforzare (a breve, a superare) gli strumenti di sicurezza visti finora: password, PIN e autenticazione a due fattori.

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 e così via. I dati biometrici sono dunque delle informazioni altamente riservate che un macchinario individua per permettere all'utente di accedere al suo account o al suo dispositivo. Per analizzare questi dati è necessario avere dei sensori biometrici.

Il sistema di riconoscimento delle informazioni biometriche di una persona viene anche chiamato AIDC (*Automatic Identification and Data Capture*).

Nei prossimi smartphone e notebook i sensori biometrici saranno sempre più usati proprio perchè la sicurezza informatica sta diventando una caratteristica fondamentale per i dispositivi e l'uso dei PIN o delle password, da soli, 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 di PIN o agli altri metodi di sblocco.

Su molti telefonini il lettore per le impronte è cliccabile e permette di aprire velocemente un'app o la fotocamera. A breve questi sensori prenderanno piede anche nei touchpad dei computer portatili.

Cancellare la Cronologia

Mentre navighi in Internet, il tuo browser (Google Chrome, Edge, Firefox e così via) conserva la cronologia dei siti visitati e, cioè, un elenco di tutte le pagine web che hai visitato.

È un strumento utile se, anche a distanza di tempo, vuoi tornare su una pagina che ricordi abbia notizie che ti interessano, anche se non ricordi l'indirizzo (URL) del sito.

Indirettamente, però, può rappresentare una minaccia per la tua privacy: chiunque abbia accesso al tuo computer, infatti, potrà conoscere le pagine che hai visto di recente.

Valutandone i pro e i contro, potresti decidere di cancellare la cronologia ogni volta che navighi o, a seconda dei casi, ogni settimana, ogni mese e così via.

Ogni browser ha un apposito comando nella finestra delle opzioni.

Impariamo a gestirlo nel modulo dedicato alla navigazione in rete.

1.2 Il concetto di privacy

Abbiamo visto che gli attacchi informatici sono finalizzati alla manomissione dell'hardware e/o alla sottrazione di informazioni sul tuo conto.

Nel primo caso, può succedere, ad esempio, che sia danneggiato irrimediabilmente il sistema operativo o l'hard disk del tuo PC; dovrai comprarne un altro. Nel secondo caso, è possibile che un estraneo entri nella tua casella di posta elettronica.

Quale dei due danni è più grave o pericoloso?

1.2.1 Problemi connessi alla sicurezza dei dati personali

Potrai pensare che sia meglio che qualcuno sbirci le tue conversazioni piuttosto che spendere diverse centinaia di euro per mettere a posto il PC.

Probabilmente questa idea deriva dal fatto che siamo oramai abituati alla continua erosione che molte tecnologie fanno, di continuo, della nostra sfera personale.

Siamo consapevoli del fatto che molte delle nostre attività online vengono osservate e registrate e confidiamo nel fatto che ciò sia fatto solo per supervisione o statistica. Ma non è sempre così.

1.2.2 La social engineering

Nel prossimo paragrafo vedremo quali sono gli strumenti più diffusi per carpire informazioni sul tuo conto.

Qui accenniamo a tattiche molto più sofisticate che sempre più hacker stanno mettendo in campo per riuscire a trafugare dati e informazioni personali di ogni genere. Si definiscono *social engineering* (ingegneria sociale) e sono a metà tra psicologia e ingegneria.

Un ingegnere sociale – un hacker che mette in atto queste tecniche – studia il comportamento online della vittima e ne conquista la fiducia, durante conversazioni che indirizza conoscendo quali sono i suoi argomenti preferiti.

La *social engineering* è una manipolazione psicologica che induce chi ne è vittima a comportarsi in una determinata maniera o rivelare informazioni personali senza rendersene realmente conto.

Si tratta di attività molto più articolate dei normali malware ma può portare a risultati molto più fruttuosi, in termini di acquisizione di notizie personali.

È chiaro che tale tecnica può essere utilizzata anche nei confronti, ad esempio, dei dipendenti di un'azienda di cui si voglia carpire i segreti organizzativi o produttivi.

Si discute molto del lavoro che sembra stiano facendo i pubblicitari di grandi aziende: monitorando le nostre attività online, creano profili delle nostre preferenze, per organizzare campagne commerciali o offerte ad hoc. Può sembrare una cosa buona e utile per tutti… si tratta di valutare i pro e i contro, in concreto, per i cittadini. Il tema della privacy è molto dibattuto e complesso.

1.2.3 Il furto d'identità

Altra attività che rientra nella *social engineering* 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; vediamone alcune.

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. Spesso queste informazioni viaggiano in rete in chiaro e non in modalità protetta.

Un crescente numero di utenti, inoltre, sta fornendo un'elevata quantità di dati personali a blog, siti di chat, social networks e questo ha attratto molto l'attenzione di hacker e malintenzionati. Conoscendo i dati immessi in questi sistemi, è possibile trovarne altri!

Ci sono, poi, malware pensati appositamente per questo: *phishing*, *vishing*, *pharming*, *sniffing*. Ne parleremo diffusamente tra breve.

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 di terzi.

Come prevenire il furto d'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:

- Proteggi il 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, alcuna password, alcun 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 (di biblioteche, internet point, internet café, e così via).
- 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.

Come capire se la propria identità è stata rubata

- Controlla frequentemente il tuo conto corrente per verificare inusuali o inaspettati accrediti/prelievi.
- Verifica bene come stanno le cose se ricevi fatture di prodotti o servizi che non hai mai richiesto o non ricevi servizi, resoconti e/o fatture che hai richiesto e/o attendevi.
- La carta di credito non funziona.

In questi casi è sempre bene sospettare un furto di identità. In tal caso, devi:

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

Se sei certo di essere una vittima di furto, è necessario:

- Denunciare l'accaduto al Pronto Intervento (112 per i Carabinieri, 113 per la Polizia di Stato).
- Recarsi, poi, negli uffici dell'Autorità di Polizia Giudiziaria e presentare la 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.

1.2.4 Come difendersi dagli attacchi di ingegneria sociale

Questa fattispecie è emblematica del fatto che tenere un certo comportamento online è il modo migliore per evitare problemi anche gravi.

Proteggi le tue transazioni online utilizzando firewall, antivirus e antispyware, e nascondendo la tua connessione wireless domestica. 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.

Crea password complesse, ne abbiamo già parlato. Tieni segreti password e PIN (numeri di identificazione personale) e non inviarli mai per email o con messaggi istantanei. Devi utilizzare password diverse per ognuno dei tuoi account; se utilizzi sempre la stessa, chiunque se ne impadronisca, metterà 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, messaggi istantanei o pubblicità pop-up, potresti essere portato su siti legittimi solo in apparenza ma, in realtà, 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 un computer pubblico o condiviso, oppure su dispositivi come PC portatili e 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 alcunchè, chiedi informazioni ai tuoi genitori, al tuo docente o a un amico che ne sappia più di te.

1.3 Misure per la sicurezza dei file

1.3.1 Attivare e disattivare macro

Nei file di Office (Word, Excel e così via), le macro sono delle scorciatoie che, tramite la pressione di combinazioni di tasti e clic del mouse, ti consentono di eseguire in modo veloce attività frequenti.

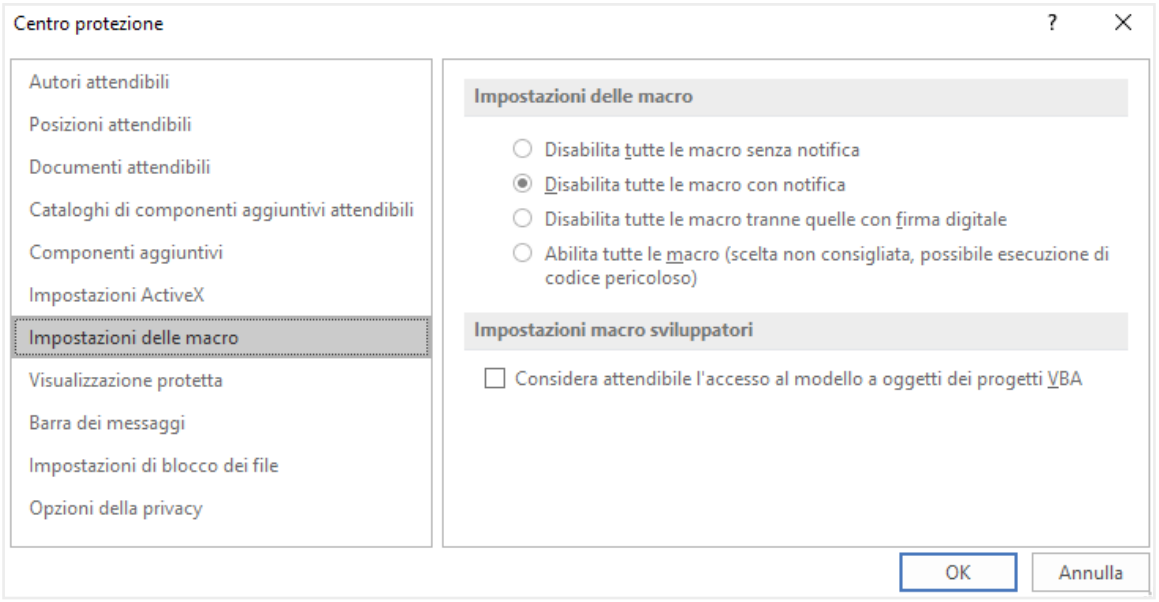
Facciamo un esempio: lavori in un'azienda e, alla fine di ogni mese, devi presentare al responsabile della contabilità un report, in Excel, con l'indicazione dei pagamenti ricevuti dai clienti; potresti decidere di segnare di rosso e in grassetto tutti i clienti morosi: i clienti, cioè, che dovendo pagare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

Molte macro vengono create da sviluppatori di software e sono, quindi, 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 inviartela in allegato in una mail.

1.3.2 Cambiare le impostazioni delle macro

1. Apri un file di Office.
2. Clicca su scheda *File* > *Opzioni* > *Centro di protezione*.
3. Clicca sul pulsante *Impostazioni Centro di protezione*.
4. Nella finestra *Centro di protezione*, clicca su *Impostazioni delle macro* e scegli tra le opzioni disponibili:
   - *Disabilita tutte 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 no.
   - *Disabilita tutte le macro tranne quelle con firma digitale*: l'opzione abilita la stessa funzione della precedente; tuttavia, la macro viene eseguita automaticamente se riporta la firma digitale di un autore attendibile.
   - *Abilita tutte le macro*: se abiliti questa opzione, verranno eseguite tutte le macro dei tuoi file. Non ti consigliamo di attivarla: con questa impostazione il computer è vulnerabile all'attacco di codice potenzialmente dannoso.



1.2 | Finestra di dialogo *Centro protezione*

Per lo stesso motivo, ti consigliamo, inoltre, di non attivare l'opzione *Considera attendibile l'accesso al modello a oggetti dei progetti VBA*.

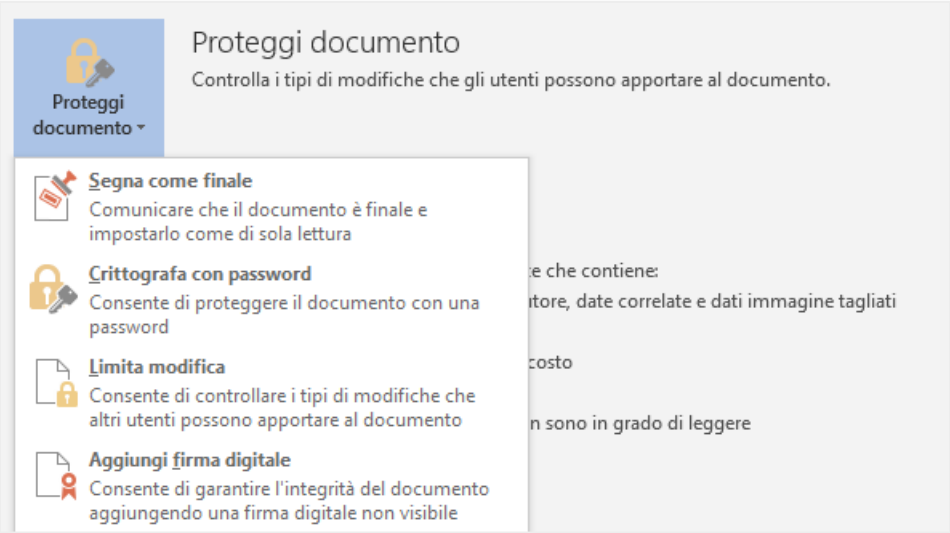
1.3.3 Cifrare e impostare password per la sicrezza dei nostri file

Ci sono diversi modi per rendere inaccessibili i tuoi file: per fare in modo, cioè, che nessuno, pur accedendo al tuo PC, possa aprirli, visualizzarli e manometterli.

Il primo è quello di attivare l'opzione *Nascosto,* nella finestra di dialogo *Proprietà*. Ne abbiamo parlato diffusamente nel paragrafo 3.3.1 del modulo *I fondamenti dell'ICT*.

Un secondo metodo è quello di inserire una password: quando si clicca sul file per aprirlo, si attiva una finestra in cui è necessario inserire la combinazione alfanumerica che hai scelto.

1. Apri un file di Office.
2. Clicca su scheda *File* > pulsante *Proteggi documento*. Si aprono diverse opzioni.
3. Scegli *Crittografa con password* per aprire un'altra finestra, in cui inserire la password che sarà, d'ora in poi, necessaria per aprire il file.



1.3 | Come inserire una password per cifrare un file

Per cifrare i tuoi file, puoi usare appositi software; ce ne sono disponibili anche gratuitamente (vedi, per esempio, File decoder).

2. MALWARE

2.1 Attacchi e minacce informatiche

Purtroppo, tutte le cose che avrai potuto leggere e sapere circa i pericoli cui vai incontro navigando in Internet non sono esagerazioni.

In questo capitolo impareremo a riconoscere diversi strumenti tramite cui molti cercano di raccogliere informazioni sul tuo conto, violando la privacy, o di impadronirsi del tuo computer e utilizzarlo per altri scopi, a tua totale insaputa.

2.1.1 I malware

L'espressione *malware* deriva dalla contrazione delle parole inglesi *malicious* e *software* e indica un qualsiasi programma creato allo scopo di causare danni a un dispositivo su cui viene eseguito e sui dati che vi sono immagazzinati. Ce ne sono di due tipi:

- di tipo parassitario, trasmessi mentre il computer è in funzione;
- del settore d'avvio, trasmessi quando colleghi e tenti di avviare un disco esterno: il virus si aggancia in memoria come se fosse un driver di una periferica ed è difficilissimo da rimuovere.

Il primo malware, conosciuto come *Brain*, fece la sua apparizione nel 1986.

Allora i computer erano davvero molto pochi rispetto a oggi: la propagazione era poi limitata dal fatto che, per infettare un PC, era necessario che vi fosse materialmente inserito un *floppy* infetto.
Brain costituì una vera ispirazione per gli appassionati di *software* che, da allora, iniziarono a gareggiare per dimostrarsi più bravi degli altri nell'accedere a sistemi governativi o sviluppare programmi capaci di diffondersi rapidamente in tutto il mondo (il primo ad avere grande diffusione fu denominato *Morris*.
Fino al 2000, i malware non erano molto dannosi (le finalità erano, appunto, goliardiche) ed erano facilmente rimovibili.
Con il nuovo millennio, le cose sono cambiate di molto: l'aumento esponenziale di connettività e numero di utenti, ha indotto molti a utilizzarli per fini criminali.

2.1.2 I malware più diffusi

Il *virus* (termine con cui generalmente, ma erroneamente, vengono indicati tutti i malware) è un piccolo programma, che contiene una sequenza di istruzioni in grado di attivare automaticamente azioni che danneggiano un computer.

Agisce in maniera simile a un virus biologico: è pericoloso, quindi, per la sua tendenza a creare epidemie: parte delle istruzioni del programma infettivo sono deputate alla riproduzione di copie di sé stesso. Dopo la fase riproduttiva, i virus informatici iniziano a svolgere attività di diversa natura e, anche quando non sono direttamente dannosi per il sistema operativo che li ospita, comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.
In generale, un virus danneggia direttamente solo il software della macchina che lo ospita, anche se può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU, fermando la ventola di raffreddamento.

Il *worm* (letteralmente traducibile con la parola *verme*) rallenta il sistema attivando operazioni inutili e dannose.

Il *trojan horse* è un programma che l'utente scarica perché ha funzionalità utili e desiderate, ma che, se eseguito, avvia, a sua insaputa, (da qui il richiamo al cavallo di Troia), istruzioni dannose per i file.

I *dialer* gestiscono la connessione a Internet tramite la vecchia linea telefonica. Possono essere utilizzati per modificare il numero telefonico digitato dall'utente, per chiamare, ad esempio, numeri a tariffa speciale, in modo da trarne profitto illecitamente.

È molto probabile che il tuo PC sia contagiato da un *hijacking* se, digitando l'URL di un sito Internet, vieni indirizzato a un altro oppure se la pagina predefinita del tuo browser (Google, ad esempio) è diventata qualcos'altro.

La *zip bomb* è un programma che disattiva le difese del PC per consentire a un altro virus di infettarlo. È un archivio compresso malevolo che rende inutile il programma che lo legge: per eliminarlo, prima che apra la strada ad altri malware, bisognerebbe cancellare il file senza aprirlo, eseguirlo o decomprimerlo.

Gli *spyware* sono usati per spiare le informazioni del sistema sul quale sono installati (abitudini di navigazione, password e altri dati sensibili) che sono quindi acquisite da un terzo interessato ma non autorizzato. Ne abbiamo accennato nel paragrafo dedicato al furto d'identità.

Essendo una tipologia molto diffusa, vediamo come funzionano in maniera un po' più attenta.

Gli spyware

- Il male intenzionato fa *phishing* quando invia e-mail, con campi da compilare, link o finestre a comparsa, con l'intento di carpire i dati che l'utente dovrebbe inserire per rispondere all'invito o di farlo connettere a specifici siti. Fa leva sul fatto che un utente inconsapevole o distratto possa decidere di comunicare i propri dati o cliccare su un link, credendo si tratti di una comunicazione importante.

- Il *vishing* è l'ultima evoluzione del phishing, legata all'utilizzo del VoIP (le telefonate via internet). Può succedere che il cyber criminale si spacci per una banca, facendo addirittura comparire il vero numero dell'istituto di credito sul display dell'utente, spingendolo, 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 detti, appunto, *sniffer*, volta a monitorare e diagnosticare problematiche di rete; può essere utilizzata in modo fraudolento per intercettare informazioni sensibili, come login e password di accesso a un determinato servizio.

Come si diffondono gli spyware

Gli spyware si diffondono in due maniere:

- Possono essere installati automaticamente sul tuo PC, attraverso siti Internet infetti;
- Puoi installarli manualmente (ma in maniera involontaria), scegliendo di utilizzare programmi gratuiti (*software freeware*) che riescono facilmente a infettare PC che non abbiano difese sufficientemente alte.

Come riconoscere la presenza di uno spyware sul tuo PC

Quando un PC è infetto, normalmente si attivano delle azioni che, altrimenti, non si attiverebbero mai. Te ne indichiamo alcune:

- Mentre lavori, *compaiono in continuazione pop-up pubblicitari*.
- *Si sono modificate impostazioni che sei certo di non aver cambiato personalmente e non riesci a resettarle*. L'esempio più classico è la modifica della pagina iniziale del tuo browser. Anche ripristinando la tua preferita, a ogni riavvio torna quella indesiderata.
- *Il tuo browser contiene componenti aggiuntive che non ricordi di aver scaricato*. Succede spesso, ad esempio, che compaiano *barre degli strumenti* che non ti servono o non desideri che, come sopra, anche se le elimini, ricompaiono a ogni riavvio del computer.
- *Il computer è lento*. I malware non sono efficienti; non c'è alcuna necessità che lo siano: le risorse che utilizzano per monitorare le tue attività e inviare pubblicità possono, quindi, rallentare il PC e/o provocare errori del sistema operativo.

Prevenire e rimuovere uno spyware

Per difendere e disinfestare in nostro PC da attacchi malevoli in generale, dobbiamo utilizzare un programma antivirus. Ne parleremo tra poco.

Se decidiamo di stare particolarmente attenti agli *spyware*, possiamo scegliere programmi specifici, pensati proprio per difenderci da questo tipo di attacchi. Eccone alcuni:

- Ad-Aware SE Personal Edition
- Emsisoft Anti-Malware
- Malwarebytes' Anti-Malware
- HijackThis
- Norman Malware Cleaner
- Spybot - Search and Destroy
- SpywareBlaster
- Spyware Terminator
- SUPERAntispyware

2.1.3 Altre categorie di attacchi informatici: gli attacchi login

Il *thiefing* consiste nello sfruttare l'assenza di misure di protezione adeguate, per sottrarre servizi informatici: hai mai provato a connetterti alla rete wireless del tuo vicino che non s'è curato di inserirvi una password? Stavi facendo *thiefing*!

Il *keylogger* è un sistema che consente di intercettare tutto quello che un utente digita su una tastiera. È molto usato per appropriarsi indebitamente dei dati digitati sulle tastiere degli sportelli bancomat. Esistono due tipi di *keylogger*:

- *hardware*: dispositivi che vengono collegati al cavo di comunicazione tra la tastiera e il computer o all'interno della tastiera;
- *software*: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

2.2 Gli strumenti di difesa

L'unico computer totalmente sicuro e a prova di hacker è quello spento, non collegato a Internet e chiuso a chiave in una cassaforte!

I software maligni vengono diffusi principalmente tramite Internet (e-mail, condivisione di file in reti P2P e per mezzo dei siti Web non attendibili), ma possono essere entrare nel tuo PC anche attraverso i dispostivi di memoria esterni, come le chiavette USB.

Il principale strumento per la difesa della tua privacy e dei tuoi dati è il tuo buon senso.

Di fatto, la colpa dell'elevata diffusione di malware è da attribuire soprattutto a chi utilizza il PC: troppo spesso non ci curiamo delle più basilari misure di sicurezza, anche se immediatamente disponibili.

Uno di questi è il firewall; impariamo a impostarlo nel modulo dedicato ai fondamenti dell'ICT. Qui vediamo come funziona tecnicamente.

2.2.1 A cosa serve il firewall

Se ben configurato e usato correttamente, permette di:

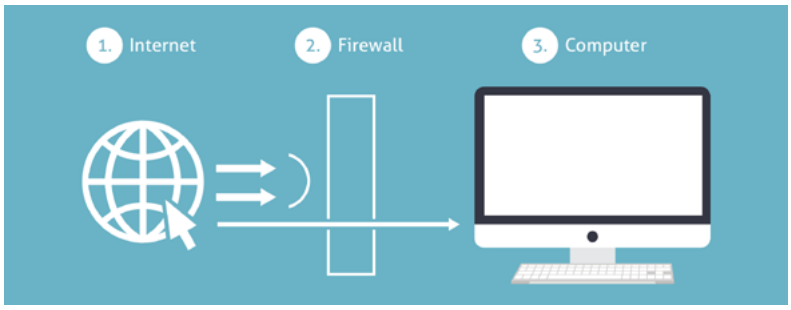
- bloccare i malware, anche non conosciuti, prima che questi entrino nel computer;
- bloccare all'interno del PC i malware che siano riusciti a entrare, evitando così che possano infettare altri dispositivi eventualmente collegati.

Il firewall:

- impedisce a un malware di infettare la macchina prima che venga individuato dall'antivirus,
- nasconde il computer durante la navigazione, diminuendo al minimo i rischi.

Per comprendere bene come funziona, facciamo un esempio molto semplice: il firewall funziona come una dogana che controlla:

- il traffico di rete che proviene dall'esterno;
- il traffico dei dati generati dal PC e inviati all'esterno, permettendo soltanto quello effettivamente autorizzato.



2.1 | Funzionamento del *firewall*

Come funziona tecnicamente

Dobbiamo fare una breve premessa circa i protocolli che consentono ai computer in rete di riconoscersi e comunicare.

Facciamo riferimento al protocollo più utilizzato in Internet, il TCP/IP (*Transport Control Protocol/Internet Protocol*).

In un network basato sul TCP/IP, ciascun computer:

- è identificato in modo univoco da un *indirizzo IP* (costituito da quattro *ottetti*, del tipo *aaa.bbb.ccc.ddd*);
- comunica con altri sistemi, scambiando messaggi sotto forma di *pacchetti* (detti *datagrammi*).

Affinchè ci sia una comunicazione, quindi, è necessario che in ogni computer connesso ci siano due elementi:

- l'*indirizzo IP* che, come un numero di telefono, rende riconoscibile e contattabile il computer da un altro in rete,
- una *porta di comunicazione* (un numero) che serve a individuare l'applicazione usata per comunicare (il numero di porta del servizio http è 80, ad esempio).

Una volta instaurata la connessione, il *firewall* inizia a svolgere la sua funzione di *filtro*, analizzando tutti i *pacchetti* che lo attraversano: saranno automaticamente bloccati tutti quelli che corrispondono al *set di regole* definito dall'utente.

Diversi tipi di firewall

Dal punto di vista del funzionamento interno, i firewall possono essere distinti in due gruppi:

- *a filtraggio di pacchetti*, più comuni e meno costosi, esaminano le informazioni contenute nella intestazione del pacchetto relativa al protocollo IP e le confrontano con il loro set di regole interno, permettendone o bloccandone il transito. Il vantaggio di questi dispositivi, oltre al costo contenuto, è rappresentato dalla velocità; ci sono, peraltro, pesanti punti deboli:
  - una certa vulnerabilità nei confronti di determinati tipi di attacco (come quelli basati sull'*IP spoofing*),
  - essendoci una *connessione diretta* tra *sorgente* e *destinazione*, una volta che il *firewall* lascia transitare un *pacchetto*, non c'è più alcuna difesa contro ogni successivo attacco portato dallo *stesso pacchetto*.
- *a livello di circuito*, forniscono un livello di protezione più elevato poiché esaminano non soltanto l'intestazione ma anche il contenuto dei *pacchetti* in transito: in questo modo, verifica sempre che il sistema di destinazione abbia effettivamente richiesto il dato in transito.

2.2.2 L'antivirus

Ci sono, poi, specifici software per la protezione dei nostri dati (DMS, IDS/NIDS).

Il più conosciuto è l'antivirus. Vediamo come funziona.

Si tratta di software ideato per:

- prevenire l'infezione,
- rilevare ed eventualmente eliminare programmi malevoli che insidiano la sicurezza dei computer.

Ce ne sono molti che rilasciano le funzioni basilari in maniera gratuita. Devi scaricarli da Internet.

2.2.3 Il funzionamento di un software antivirus

Ciascun malware è composto da un numero preciso di istruzioni, un codice costituito da una stringa di byte, detta *firma*.

L'antivirus identifica la minaccia passando al setaccio il PC, i file e la RAM: in pratica, confronta tutto ciò che è in funzione sul PC con il proprio database delle firme dei malware.

Se identifica un file contenente una di queste firme, lo blocca e segnala subito la cosa.

Le diverse parti dell'antivirus

L'antivirus è composto da diversi elementi:

- il file (o i file) delle firme contengono tutte le firme dei virus conosciuti;
- il file binario ricerca il virus all'interno dell'elaboratore. Questo componente è l'antivirus vero e proprio;
- il file binario che effettua gli *update* (aggiornamento) del file delle firme e dei binari dell'antivirus.

2.2.4 Scansione del sistema

I diversi tipi di scansione disponibili

La scansione è il processo di analisi dell'antivirus. Si può impostare la scansione all'avvio del computer o effettuarla in qualunque altro momento.

L'antivirus utilizza molte risorse del computer per funzionare: se viene avviato automaticamente ogni volta che il computer viene acceso, può comportare un forte rallentamento, soprattutto nelle fasi iniziali (perché controlla prima tutta la memoria e poi tutti i file, che rientrano nella ricerca selezionata durante la fase configurazione, su disco).

Ci sono differenti tipi di scansione.

- La *scansione completa* analizza file e applicazioni in esecuzione in tutte le unità del computer. Questo tipo di scansione è più lenta delle altre e richiede maggiori risorse del sistema operativo. Rallenta il funzionamento del computer ma consente di rilevare il maggior numero possibile di infezioni.

Esegui la *scansione completa* una volta alla settimana, programmandola nel momento più idoneo: durante le ore notturne, ad esempio.

- La *scansione su misura o personalizzata* consente di selezionare le unità e le cartelle da sottoporre a scansione.

- La *scansione rapida* verifica l'integrità dei file caricati all'avvio del sistema operativo e la memoria di sistema. Questo tipo di scansione potrebbe non individuare alcuni malware ma, comunque, informa della presenza di un virus nel caso in cui il computer sia infetto.
- La *scansione intelligente* verifica le aree più soggette a infezione.

Avanzamento scansione

Una volta avviata la scansione, visualizzi una barra di avanzamento che indica la percentuale della scansione completata fino a quel momento e il tempo rimanente per comletarla.

È possibile interrompere o mettere in pausa la scansione in ogni momento, usando le relative finestre di comando.

Antivirus real-time

L'ultima frontiera contro i malware è l'*analisi comportamentale*.

Gli antivirus più evoluti hanno un sistema, definito real-time, capace di analizzare le operazioni eseguite istantaneamente sul PC e comprendere se si svolgano in maniera corretta o, in qualche modo, allarmante.

In questa maniera, riescono a individuare file infettati che siano riusciti a eludere tutti gli altri tipi di rilevamento e scansione.

Risultati scansione

Completata la scansione, se sono state rilevate minacce, visualizzi un elenco delle infezioni e dei relativi livelli di rischio.

A questo punto, devi selezionare le *opzioni di correzione*. Puoi:

- *mettere in quarantena i file infettati*: saranno isolati in una sezione del PC da cui non si possono muovere; puoi ripristinarli in qualunque momento, se necessario;
- *rimuovere* il file in maniera permanente (senza metterlo in quarantena).

2.2.5 L'aggiornamento dell'antivirus

Se vuoi che il tuo antivirus sia efficace devi aggiornarlo in maniera sistematica.

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.

Oltre ai produttori, infatti, sono diverse le organizzazioni 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*, squadra di risposta alle emergenze informatiche).

2.3 I malware poliformi e l'euristica

Anche in questo campo, la tecnologia sta facendo passi da gigante: il confronto tra chi crea malware e chi cerca di scovarne è sempre più serrata.

2.3.1 Come funzionano i malware poliformi

L'ultima frontiera è l'*euristica*. Gli antivirus programmati con tecnologia euristica sono in grado di riconoscere anche firme *parziali* di malware, per individuarne di nuovi. Ciò avviene soprattutto in relazione ai malware definiti polimorfi.

Il malware polimorfo è in grado di nascondere il proprio codice: lo fa utilizzando una chiave diversa in ogni tentativo di infezione. È dotato di un motore, anch'esso cifrato, che modifica in maniera casuale la procedura che attiva l'infezione.

Riassumendo, abbiamo imparato che:

- l'antivirus è in grado di eliminare soltanto i malware che riconosce, ossia quelli già presenti nel suo database,
- i nuovi malware (quelli non riconosciuti e quelli che non sono ancora stati scoperti) possono passare completamente inosservati e non essere rilevati.

L'aggiornamento del tuo antivirus serve proprio a rimpinguare il suo database, in modo tale che almeno tutti i malware già riconosciuti (cioè già immessi nella lista del database online del software) non diventino mai un problema serio per il tuo PC.

Oggi tutti gli *antivirus* si aggiornano automaticamente, non appena è disponibile una connessione online.

Da quando la Symantec ha introdotto il sistema automatico *live-update* per il suo antivirus *Norton*, è diventato davvero semplice aggiornare questi programmi.

3. LA SICUREZZA DELLE RETI

Abbiamo introdotto il tema nel modulo dedicato ai fondamenti dell'ICT. Riprendiamo il discorso per valutare altri punti di vista.

3.1 La rete e le connessioni

Il termine generico *rete* indica un insieme di entità (oggetti, persone, ecc.) interconnesse le une alle altre.

3.1.1 Rete e networking

In informatica, si definisce rete un gruppo di computer collegati fra loro in modo da scambiare informazioni sotto forma di dati: è questo il sistema tramite cui, in una rete informatica, è possibile condividere e far circolare elementi *immateriali* tra tutti i dispositivi connessi.

Rete (in inglese, *network*)	Attuazione di una rete (*networking*)
Insieme di computer e periferiche connesse le une alle altre: due computer connessi tra loro costituiscono una *rete minimale*.	Strumenti e compiti che permettono di collegare diversi computer tra loro, affinché possano condividere delle risorse, *in rete*.

I vantaggi del *networking* sono evidenti:

- Diminuzione dei costi, grazie alle condivisioni di dati e periferiche
- Standardizzazione delle applicazioni
- Accesso ai dati in tempo reale
- Comunicazione e organizzazione più efficace.

3.1.2 Le reti

È possibile classificare le reti informatiche a seconda della dimensione.

Nel modulo dedicato ai principi dell'ICT, abbiamo parlato di rete LAN, *Limited area network* (con estensione limitata), WAN, *Wired Area Network* (si estende su un territorio che può essere molto ampio) e MAN (rete di estensione intermedia).

Ogni rete è costituita, comunque, dai seguenti elementi:

- *Server*: sono i computer che conservano i dati cui possono accedere i client.
- *Client*: sono i computer degli utenti che accedono ai dati forniti dal server di rete.
- *Supporto di connessione*: è il sistema che collega i computer coinvolti.
- *Dati condivisi*: sono i file resi accessibili dal server ai client collegati.
- *Stampanti e altre periferiche condivise*: risorse utilizzabili dagli utenti della rete.

3.1.3 LAN

A casa o in ufficio è ormai normale avere più computer collegati in rete; si tratta, normalmente, di reti LAN.

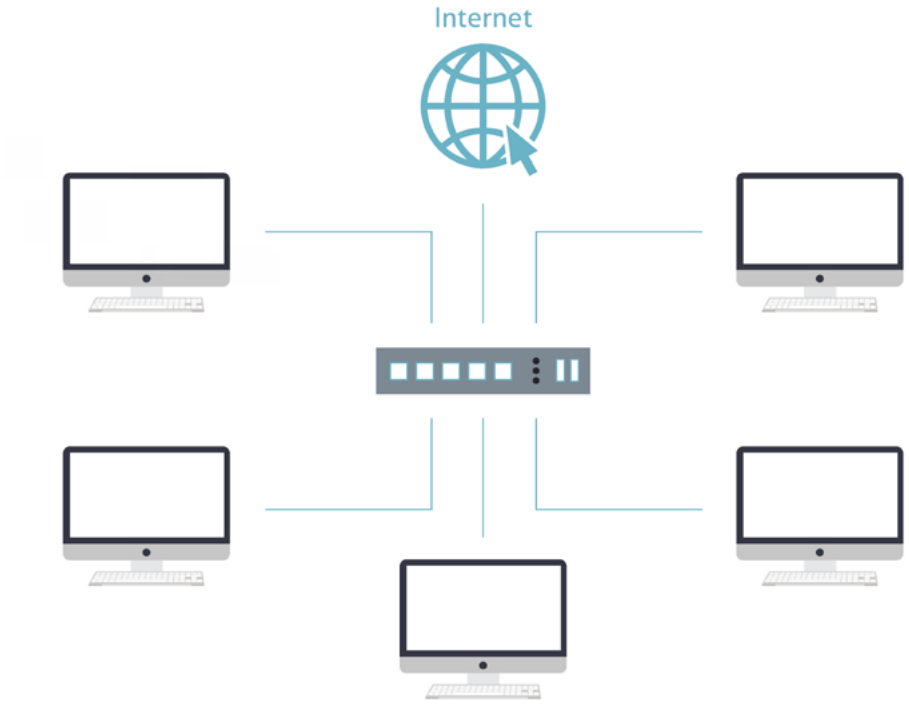
Qualsiasi dispositivo (server, computer, laptop, stampante, televisore, hard disk, NAS) può diventare *nodo* di una LAN e condividere tutte le proprie risorse con gli altri nodi/dispositivi. Se, ad esempio, nella nostra LAN è presente una stampante, tutti gli utenti connessi potranno utilizzarla dalla propria postazione.

Ce ne sono di diversi tipi. Vediamo vantaggi e svantaggi di ognuno.

LAN a stella

È il tipo più semplice: tutti i nodi sono collegati a un dispositivo centrale (*centrostella*). I dati tra i vari nodi viaggino spediti ed è poco probabile che le comunicazioni siano intercettate.

Dall'altro lato, il *centrostella* sarà spesso oberato di lavoro, dovendo smistare tutti i dati condivisi; in caso di sua rottura, l'intera rete smetterà di funzionare.

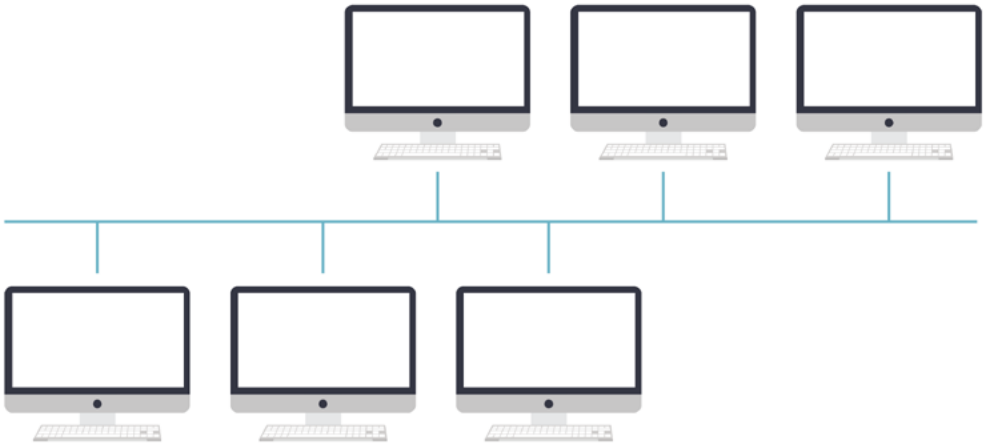


LAN a stella

LAN a bus

Tutti i nodi collegati sono agganciati direttamente al medesimo *cavo fisico*: è facile e poco costosa da realizzare ma è anche poco affidabile.

I dati che viaggiano sull'unico canale di comunicazione sono infatti facilmente intercettabili da qualsiasi altro *nodo* della rete e, inoltre, è molto complicato trovare il punto preciso di un eventuale guasto.

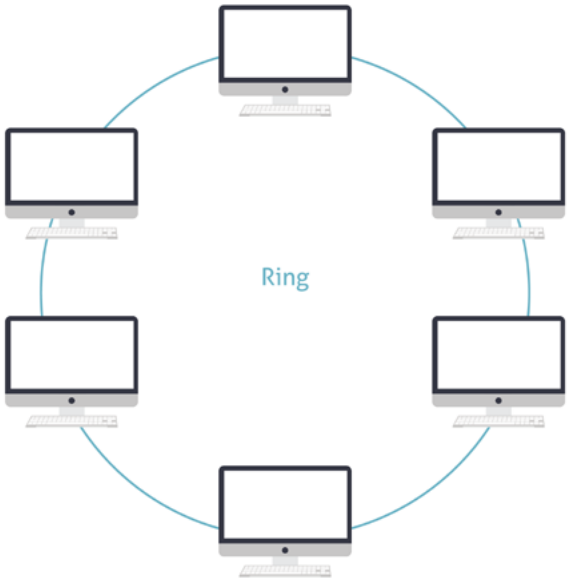


LAN a bus

LAN ad anello

È un esempio di rete *peer-to-peer*: tutti i nodi possono ricoprire sia il ruolo di *server* che di *client*, essendo collegati in fila; l'ultimo si dovrà collegare al primo, chiudendo il cerchio.

Il passaggio di dati da un nodo all'altro è regolato da un particolare messaggio, detto *token*: un nodo in possesso del *token* è autorizzato a trasmettere dati a uno dei due nodi collegati (quello che lo precede o quello che lo segue).



LAN ad anello

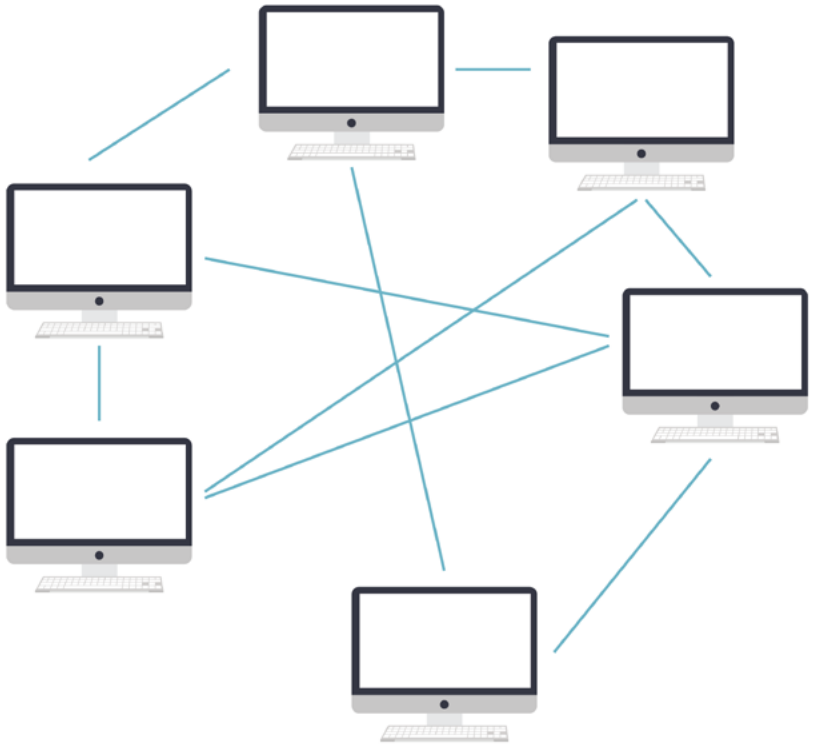
Una volta terminata la trasmissione dei dati, il nodo passerà il testimone (il *token*) a un nodo limitrofo: se questo ha dei dati da trasmettere, si attiva; diversamente, passerà subito il token al nodo successivo. Anche questa tipologia presenta problemi di affidabilità: i dati sono facilmente intercettabili e nel caso di rottura di uno dei nodi la comunicazione si ferma.

LAN mesh

Anche la LAN *a maglia* è un esempio tipico di connessione p2p: non esiste un ordine gerarchico tra i nodi, che:

- possono comportarsi, a seconda dei casi, come *server* o *client*;
- sono collegati a un numero variabile di altri nodi, senza seguire uno schema preciso.

In questo caso, la rottura di un nodo non comporta l'interruzione della comunicazione: esisterà sempre un percorso alternativo che permetterà di aggirare l'ostacolo e portare a termine la comunicazione.



LAN mesh

3.1.4 Vulnerabilità delle reti

Tutti i sistemi che abbiamo visto sono vulnerabili: possono, cioè, essere attaccati da malintenzionati che vogliano manometterle o acquisirne i dati condivisi.

Gli attacchi possono provenire da:

- utenti che fanno parte della rete ma che non si prevede possano accedere a tutti i dati scambiati: in questo caso, potrebbero trafugare o anche solo visualizzare informazioni private, senza autorizzazione (attacchi interni);
- malware, soprattutto se la rete è connessa a Internet, (attacchi esterni);
- aziende, persone, fornitori e clienti possono accedere a una rete aziendale con cui entrano in contatto e acquisire dati senza autorizzazione (Stakeholder).

3.1.5 Ruolo e compiti dell'IT manager, nel campo della sicurezza

Normalmente queste reti sono gestite da un *amministratore di sistema* (IT manager) che deve riconoscere la natura di questi attacchi e mettere in pratica le giuste contromisure.

Per garantire la sicurezza della rete, quindi, l'IT manager deve pianificare e attuare una serie di interventi integrati e finalizzati a:

- difendere i singoli dispositivi connessi alla rete (tramite il firewall e l'aggiornamento dell'antivirus);
- proteggere la rete nel suo complesso;
- proteggere i dati memorizzati nei database.

3.2 Navigare sicuri con le reti wireless

Il Wi-Fi è il modo più comodo di creare una rete: se a casa, ad esempio, ha PC in diverse stanze, potrai collegarli senza stendere cavi dappertutto!

3.2.1 L'importanza della password nel Wi-Fi

Se la tua rete di casa è collegata in Wi-Fi, c'è il concreto rischio che uno sconosciuto qualunque possa collegarvisi per manipolare i file, utilizzare le eventuali stampanti condivise e utilizzare la tua connessione a Internet.

In pratica, se una rete wireless non è protetta da password, chiunque, nelle vicinanze, potrebbe collegarsi senza alcuna difficoltà.

3.2.2 Diversi tipi di protezione

In realtà, per un esperto non è difficilissimo violare la password del Wi-Fi. Ci sono, infatti, diversi programmi che consentono di aggirarla e acquisire sufficienti dati per accedere, ad esempio, alla posta elettronica.

Ciò detto, di certo, l'utilizzo di una password scoraggerà la maggior parte degli estranei che rivolgeranno la loro attenzione a reti meno protette.

Aggiungiamo che, nel tempo, gli sviluppatori di tecnologie Wi-Fi hanno creato vari protocolli di sicurezza per le reti wireless. Vediamo le differenze tra i protocolli WEP, WPA e WPA2

Questi protocolli sono stati creati dalla WiFi Alliance, un'organizzazione formata da circa 300 industrie leader nel settore e nata nel 1999 con lo scopo di promuovere l'adozione di un unico standard per la banda larga senza fili nel mondo. È inoltre proprietaria del trademark Wi-Fi.

WEP (Wired Equivalent Privacy)

Viene dichiarato standard per la sicurezza Wi-Fi nel settembre del 1999, quando si sostiene che riesce ad assicurare lo stesso livello di sicurezza delle reti cablate.

In realtà, possiede falle di sicurezza ben conosciute che lo rendono facile da sorpassare, essendo comunque difficile da configurare. Nonostante lo sviluppo costante di questo protocollo, rimane ancora altamente vulnerabile, tanto che la WiFi Alliance lo ha abbandonato definitivamente nel 2004.

WPA (Wi-Fi Protected Access)

Il protocollo WPA è il risultato del potenziamento/miglioramento del WEP. È stato adottato formalmente nel 2003, soprattutto perché compatibile con i dispositivi che utilizzavano il WEP.

Ha due modalità:

- la modalità *personal* è adatta alle reti domestiche: una volta impostata una password nel router wireless o nell'access point, tutti coloro che vogliono utilizzare quella determinata rete Wi-Fi 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 Wi-Fi. Al momento della connessione, ogni utente inserisce la propria username, senza password. Il sistema di criptazione delle chiavi di accesso lavora in backgroud, assegnandone automaticamente una a ogni utente per ogni sessione.

Questo protocollo, dipendendo molto dalla vecchia tecnologia WEP ed essendo compatibile con lo stesso, è risultato essere molto vulnerabile alle intrusioni.

WPA2

L'introduzione dello standard di criptazione AES (*Advanced Encryption Standard*, certificato dal governo americano) ha consentito di fare un importante salto di qualità nel settore.

Il protocollo WPA2 è il risultato dell'inserimento del nuovo standard nel vecchio protocollo; ci sono miglioramenti continui, indispensabili per superare i difetti che ancora derivano dal sistema originario (WEP).

Persiste la distinzione tra le modalità *personal* e *enterprise*.

Ovviamente il WPA2 è il protocollo più sviluppato dei tre presentati: c'è sempre la possibilità che venga hackerato, ma sicuramente rallenta i tempi dell'attacco.
Ricorda, quindi, di impostare il protocollo WPA2, durante il setup iniziale del tuo router. Molto spesso, infatti, i router sono impostati di default con il protocollo WEP che ora sappiamo essere il meno sicuro.
Fai questa verifica per controllate di non aver lasciato il router completamente esposto all'esterno, senza criptazione e password!

3.2.3 Cos'è e come funziona l'hotspot

Centri commerciali, stazioni, aeroporti, bar, centri pubblici ecc. utilizzano la tecnologia Wi-Fi per offrire ai propri clienti (o ai cittadini, in generale), connettività a Internet gratuita, tramite l'attivazione di un hotspot.

L'hotspot è un *punto di accesso* a internet che, sfruttando il Wi-Fi, è a disposizione dei device di tutti coloro che sono nelle vicinanze.

Per creare una rete di questo tipo, è necessario contattare a una società che produce *gateway* specifici (normalmente sono autoinstallanti) e, nella maggior parte delle volte, disporre di una linea telefonica ADSL.

L'esercente che offre il servizio, di norma, imposta una password di accesso.

Sicuramente ti sarà già capitato, ad esempio, in aeroporto, di accedere a una rete di questo tipo: con il tuo smartphone, avviando il browser, accedi a una pagina da cui puoi richiedere al gestore del servizio una password. Serve per autenticarti.

Dopo l'autenticazione, puoi navigare liberamente.

Questo iter è una forma di tutela per chi mette a disposizione la linea che, così, 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).

Hotspot personale: il tethering

Anche uno smartphone può fungere da hotspot (in questo caso si parla di *tethering*).

È uno strumento molto utile quando sei in un posto in cui non c'è connettività oppure costa troppo; potrai accedere a Internet sfruttando, ad esempio, la connessione di un amico.

Facciamo il caso che abbia un iPhone X. Deve cliccare su *Impostazioni* > *hotspot personale* > *attivare la funzione*.

A questo punto cerca le connessioni disponibili sul tuo smartphone. Scegli quella del tuo amico: si apre una casella in cui devi inserire la sua password di accesso al servizio. E il gioco è fatto.

Per disconnetterti, ci sono tre possibilità:

1. Ti allontani dallo smartphone del tuo amico.
2. Disattivi il WI-Fi sul tuo smartphone.
3. Il tuo amico disattiva la funzione *Hotspot* sul suo smartphone.

Bisogna fare attenzione a eventuali costi aggiuntivi, non molto frequenti ma, con alcuni gestori, comunque presenti.

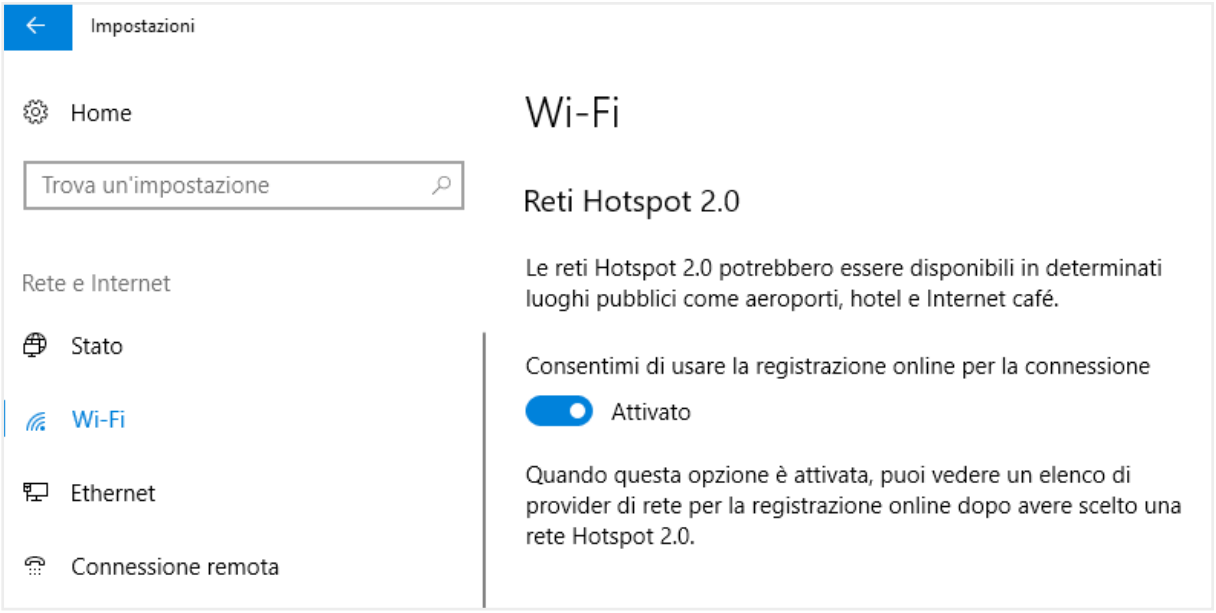
L'hotspot 2.0 di Windows 10

Windows 10 consente di accedere a un nuovo sistema di hotspot, denominato 2.0.

Se sei al PC o hai un portatile, per connetterti è chiaramente necessario che tu abbia una scheda Wi-Fi; gli ultimi modelli ne sono forniti; se il tuo PC non ce l'ha, puoi utilizzare una pen drive che svolge questa funzione.

Per attivare la ricerca di questo tipo di hotspot, apri *Impostazioni* > scegli *Rete e Internet* > *Wi-Fi* dall'elenco a sinistra e attiva la funzione *Consentimi di usare la registrazione online per la connessione*.

Quando proverai ad accedere per la prima volta a un hotspot 2.0, Windows ti mostrerà una lista dei fornitori. Impostato il servizio, Windows 10 si collegherà automaticamente a qualunque rete hotspot 2.0 supportata.



3.1 | Attivazione del servizio di connettività tramite il sistema hotspot 2.0

Ci sono già altri sistemi che supportano l'hotspot 2.0: reti di questo tipo sono accessibili anche da MacOS 10.9, Android 6.0 e iOS 7 e successivi.

Obiettivo delle reti hotspot 2.0 è quello di abilitare il roaming Wi-Fi anche per PC e laptop, in maniera molto simile all'approccio utilizzato nella telefonia mobile.

Sai cos'è il *roaming*?

Facciamo un esempio: supponiamo di avere un telefono cellulare con la connettività Wi-Fi attiva, e di trovarci in un'abitazione a due piani. C'è un accesso a Internet per ogni piano. Disponiamo, cioè, di due *access point wireless*, cablati sulla stessa rete, uno per il piano terra e il secondo per il primo piano.

Se siamo al primo piano, sul telefono saranno visualizzati entrambi gli access point ma il segnale di quello del piano terra sarà più debole, perché più distante.

La capacità di un dispositivo client di scegliere a quale access point collegarsi in base alla potenza del segnale, viene detta, appunto, *roaming*.

In sostanza, questo sistema consente anche al tuo PC di collegarsi automaticamente alla rete disponibile, senza che tu debba far nulla, così come accade per gli smartphone. Considerato il più elevato livello di sicurezza, rende superfluo il passaggio di autenticazione che abbiamo visto nel paragrafo precedente.

Le novità dell'hotspot 2.0 rispetto alle tradizionali reti WiFi

1. Già nella fase di pre-associazione all'hotspot Wi-Fi, il dispositivo client può ricevere informazioni aggiuntive che possono essere usate dal connection manager dello stesso device per migliorare il processo di selezione automatica della rete.
2. L'utilizzo degli hotspot pubblici diventa più semplice e sicuro perché il dispositivo già conosce qual è la rete Wi-Fi alla quale è possibile e *igienico* collegarsi.
3. Hotspot 2.0 favorisce gli accordi tra provider (detti roaming consortium): gli operatori di telecomunicazioni possono stringere delle intese fra di loro garantendo accesso automatico a tutti i propri clienti su hotspot Wi-Fi delle società partner mentre si è in mobilità.
4. L'utilizzo di un algoritmo crittografico WPA2 è requisito indispensabile per tutte le reti Hotspot 2.0.

In Italia siamo ancora piuttosto indietro sul versante hotspot 2.0 ma è bene che tu conosca qusta nuova tecnologia per sfruttarla, appena sarà possibile.

3.2.4 I pericoli delle reti wireless pubbliche

Dopo aver visto come fuziona la connessione Wi-Fi, vediamo adesso cosa può accadere quando ci connettiamo a una rete libera, ovvero a tutte quelle connessioni aperte che troviamo in giro, tra centri commerciali, bar, stazioni, aeroporti e così via.

Pochi resistono alla tentazione di connettersi a una rete gratuita e non criptata (che non richiede quindi una password personale e non usa alcuna crittografia durante lo scambio di pacchetti dati), risparmiando preziosi giga del proprio traffico telefonico.

Il punto è che in questi casi ci esponiamo ad attacchi di malintenzionati che possono acquisire i nostri dati personali.

Una rete Wi-Fi pubblica utilizza protocolli che sono facilmente attaccabili.

I protocolli cui ci riferiamo sono: l'SMTP (*Simple Mail Transfer Protocol*), l'IMAP (*Internet Message Access Protocol*), il POP (*Post Office Protocol*) che permettono all'utente di accedere al proprio servizio e-mail, l'SNMP (*Simple Network Management Protocol*) e l'HTTP (*Hypertext Transfer Protocol*) per navigare sulle pagine internet.

3.2.5 Diversi tipi di attacchi alle connessioni wireless

Vediamo i tipi di attacchi più diffusi.

Intercettazione o eavesdropping

Mai come in questo caso, utilizzare la parola inglese aiuta molto a comprendere di cosa si tratta. L'etimologia di *eavesdropping* è davvero evocativo e da subito l'idea di un'usanza (un malcostume) vecchio quanto il mondo.

Eaves si traduce con *gronda*, la parte del tetto che sporge dal muro esterno, da cui gocciola (*drop*) la pioggia. Quando piove, quindi, chi si appoggia al muro esterno di una casa per origliare, in caso di pioggia sarà inevitabilmente colpito dalle gocce che cadono dall'alto.

Da qui la definizione di *eavesdropper* (chi origlia) e *eavesdropping* (l'azione di origliare).

La definizione è tratta dai *Commentaries on the Laws of England*, scritti nel '700 da Sir William Blackstone, in cui si legge: Gli *eaves-dropper, ovvero coloro che ascoltano accanto ai muri o sotto le finestre, o le gronde delle case, per carpire i discorsi altrui e dunque inventare storie calunniose e malevole, sono una piaga diffusa e possono essere portati dinanzi alla corte, perseguibili e punibili con una multa.*

L'*eavesdropping* indica, appunto, l'atto del malintenzionato di ascoltare conversazioni altrui e di registrare tutte le informazioni utili (come per esempio login e password) che riesce a carpire.

Si parla, in definitiva, di una tecnica di intercettazione.

In questo contesto, ascoltare vuol dire *recupere pacchetti dati* e *leggerli* alla ricerca di tracce importanti.

Jamming

Una tecnica simile all'*eavesdropping* è il *jamming*. In questo caso, il maleintenzionato crea interferenze per rendere inutilizzabile un canale di comunicazione via radio.

Può essere causato anche incidentalmente da alcuni elettrodomestici in uso che disturbano le frequenze di trasmissione. Un caso tipico è quello dei telefoni cordless: capita spesso che disturbino le frequenze degli apparecchi che ripetono il segnale televisivo da una TV a un'altra, nella stessa abitazione.

Se attaccata in questo modo, un'intera area potrebbe cessare le comunicazioni wireless. Se si pensa a un attacco terroristico, si può comprendere bene quale possa essere la portata di tale tipo di attacco.

Normalmente, col *jamming* si dirottano le comunicazioni tra il client e il punto di accesso wireless, convogliandole su un altro punto di accesso, da cui trafugare informazioni.

Questa tecnica richiede, comunque, l'utilizzo di hardware di notevole potenza.

MITM (man-in-the-middle attack)

Il MITM è un modo più semplice di carpire informazioni: è ciò che fa chi si interpone in una comunicazione, fingendo di essere una delle 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.

L'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche a scopi fraudolenti è punibile in termini di legge con reclusione da 6 mesi a 4 anni.

4. NAVIGARE IN SICUREZZA

Vista anche la complessità tecnica del tema, non è possibile aspettarsi che ogni utente del web, prima di navigare, acquisisca le competenze necessarie per non correre rischi.

In effetti, ci sono strumenti che ci aiutano molto in questo.

I browser più moderni danno all'utente la possibilità di personalizzare i livelli di sicurezza, lasciandoci liberi di bloccare o meno determinati elementi che girano online.

4.1 Il browser e la sicurezza online

Tutti i browser hanno strumenti che ci consentono di navigare tranquillamente in Internet: sono pensati e continuamente aggiornati per difenderci sempre meglio e in maniera sempre più automatica.

Lo strumento più comune è quello che ti consente di eliminare i dati privati quali cronologia di navigazione e di scaricamento, file temporanei di Internet, password, cookie e dati per il completamento automatico.

Abbiamo visto come gestire alcuni di questi dati nel modulo dedicato alla navigazione in rete. Vediamo qui come gestire gli altri.

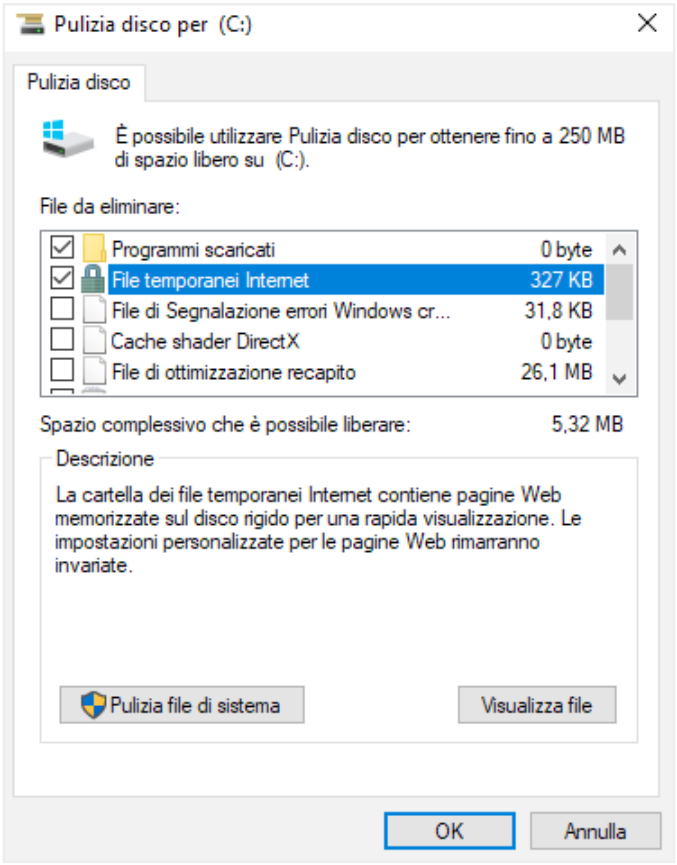
4.1.1 I file temporanei di Internet

Ti consigliamo di eliminare spesso i file temporanei che vengono salvati sul tuo hard disk per ogni azione che svolgi sul tuo PC, sia online che offline.

Possono essere utili per velocizzare alcuni operazioni (sono, in sostanza, una scorciatoria per accedere più velocemente ad alcune informazioni) ma possono essere utilizzati da terzi per carpire informazioni sulla tua navigazione in rete e, comunque, alla lunga appesantiscono il tuo sistema, rallentandolo.

Per eliminare i file temporanei:

1. Digita *Pulizia disco* in Cortana.
2. Clicca sulla prima voce dell'elenco. Si apre la finestra di dialogo *Pulizia disco*.



4.1 | Finestra di dialogo *Pulizia disco*

3. Spunta le tipologie di file che intendi eliminare. Se lasci le impostazioni di default, otterrai già una buon lavoro, eliminando anche i file temporanei di Internet.

Se intendi selezionare nuovi elementi, leggi la descrizione che puoi leggere in basso per ciascuno di essi: saprai con esattezza su cosa andrai ad agire.

4. Prima di dare il via all'operazione di pulizia, puoi anche visualizzare gli elementi che saranno eliminati, cliccando su *Visualizza file*, in basso.

Se vuoi cancellare anche altri dati di sistema, come ad esempio i file non critici di Windows Defender, clicca su *Pulizia file di sistema* e attendi qualche istante affinché il software si riavvii da solo mostrandoti la lista aggiornata dei file da rimuovere.

5. Clicca su OK e poi su *Eliminazione file* per avviare il processo.

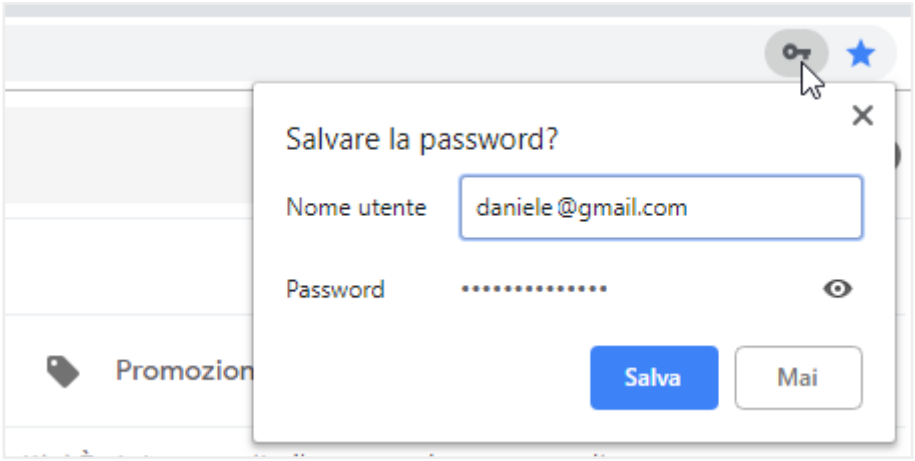
A procedura ultimata la finestra *Pulizia disco* si chiude in maniera automatica.

Puoi avviare la stessa azione tramite appositi programmi. Uno dei più efficaci è CCleaner.

4.1.2 Gestire le password

La prima volta che accedi a un tuo account (Facebook, e-mail, home banking, e così via), il browser attiva una finestra tramite cui ti chiede se intendi salvare la password.

Puoi attivare la stessa finestra anche negli accessi successivi. In Chrome, basta cliccare sull'icona della chiave. Vedi l'immagine che segue.

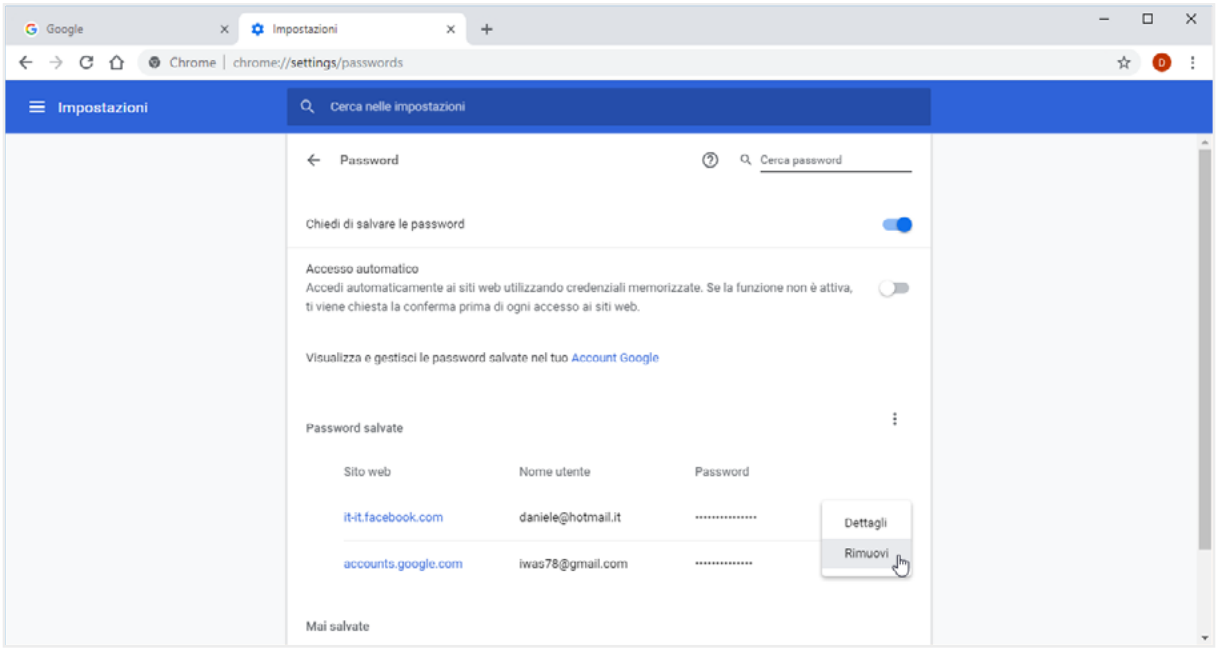


4.2 | Finestra di salvataggio della password

Ammettiamo che è molto comodo memorizzare le password: in questo modo, non dovrai più inserirle per gli accessi successivi; comprenderai bene, però, che in questo modo chiunque acceda al tuo PC potrà entrare nella tua pagina di Facebook, nella tua casella di posta e così via.

Per la tua sicurezza, ti consigliamo di non salvare mai le tue password. Se l'hai fatto, puoi comunque cancellarle. Ogni browser prevede un'apposita procedura. Vediamo quella di Google Chrome.

1. Clicca sul pulsante *Personalizza e controlla Google Chrome* (i tre puntini verticali in alto a destra).
2. Nel menu apertosi, seleziona *Impostazioni*, quindi fai clic su Avanzate nella scheda del browser.
3. Nella sezione *Persone*, clicca su password.
4. Nella sezione *Password salvate*, visualizzi l'elenco dei siti web le cui password sono memorizzate nel browser. Clicca quindi sul pulsante con tre puntini verticali in corrispondenza della password che vuoi cancellare, e seleziona *Rimuovi* nel menu apertosi.

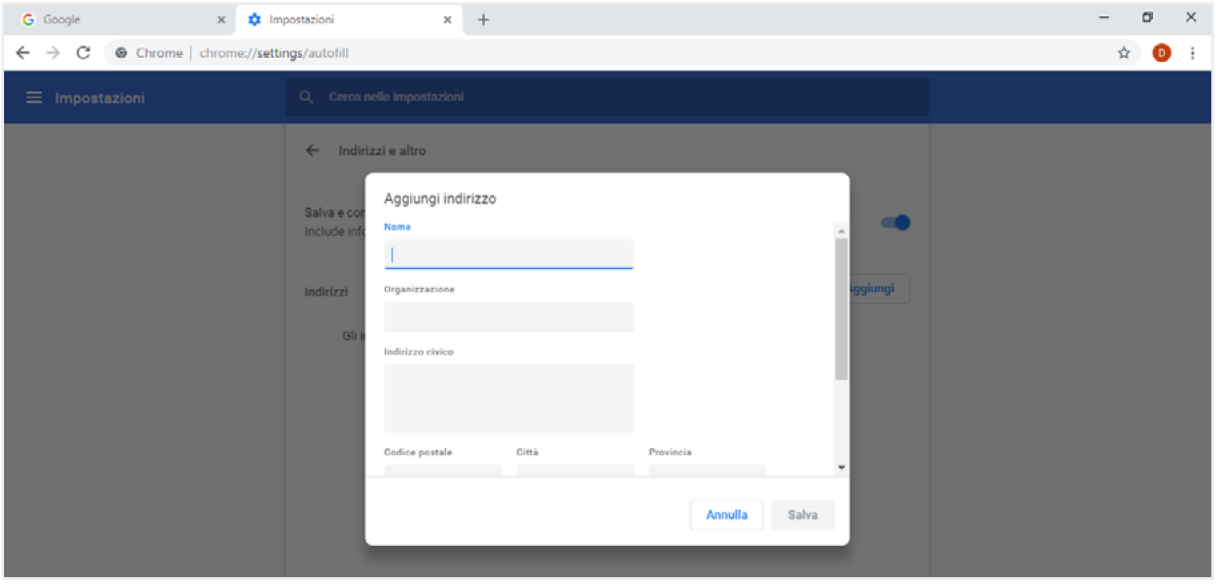


4.3 | Gestire le password

4.1.3 Compilazione automatica

Nella maggior parte dei browser puoi attivare la funzione che ti permette di compilare con un clic i *form* (moduli) online che richiedono le tue informazioni personali, come numeri di telefono, indirizzi email e indirizzi di spedizione. Queste informazioni ti verranno richieste ogni volta che, ad esempio, farai un acquisto online. Segui questi passaggi per memorizzare i tuoi dati personali in Google Chrome:

1. Clicca sul pulsante *Personalizza e controlla Google Chrome* a destra della barra degli indirizzi, e seleziona Impostazioni nel menu comparso.
2. Nella pagina web apertasi, attiva la funzione *Salva e compila gli indirizzi*, e clicca sul pulsante *Aggiungi*.
3. Nella finestra *Aggiungi indirizzo*, compila i campi come richiesto.
4. Clicca su *Salva*.

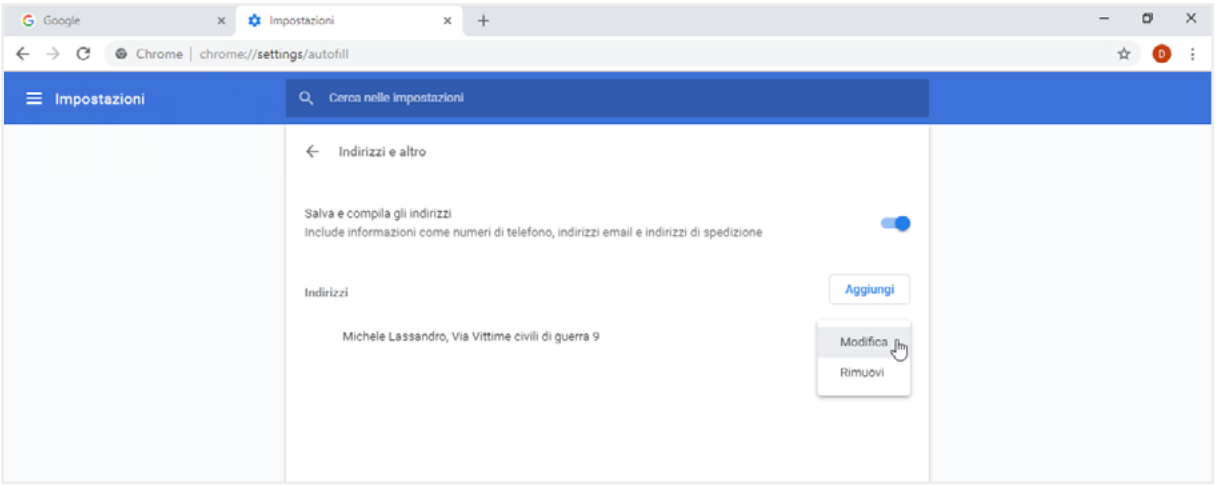


4.4 | La finestra Aggiungi indirizzo di Google Chrome

Al prossimo acquisto online, clicca nella prima casella del form, e seleziona il dato da inserire nel menu che si apre sotto la casella stessa (Daniele, nell'esempio).

4.5 | Compilazione automatica di form online

Nello stesso menu, puoi inoltre selezionare la voce Gestisci, in modo da tornare alla pagina di Chrome in cui modificare o eliminare l'indirizzo aggiunto.



4.6 | Come modificare o rimuovere l'indirizzo aggiunto in Google Chrome

Oltre ai dati personali, puoi memorizzare i dati della tua carta di credito. Nella sezione *Persone* (*Personalizza e controlla Google Chrome* > *Impostazioni*) clicca su *Metodi di pagamento*. La pagina web che si apre, attiva la funzione *Salva e compila i metodi di pagamento* e clicca sul pulsante *Aggiungi*. Nei singoli campi della finestra *Aggiungi carta*, inserisci le informazioni della carta di credito come richiesto. Per memorizzare queste informazioni, clicca su *Salva*.

La compilazione automatica è tanto comoda quanto pericolosa per la tua privacy. Vale quindi lo stesso discorso fatto quando abbiamo spiegato come si gestiscono le password.

4.1.4 I Codici attivi

L'avvento del Web Design ha reso molto più gradevoli (*frendly*, si dice) i siti web: gli esperti di grafica inseriscono specifici codici (*script*) per aumentarne le funzionalità o inserire animazioni (esempi classici sono i *menu a tendina* o la verifica del corretto inserimento della mail).

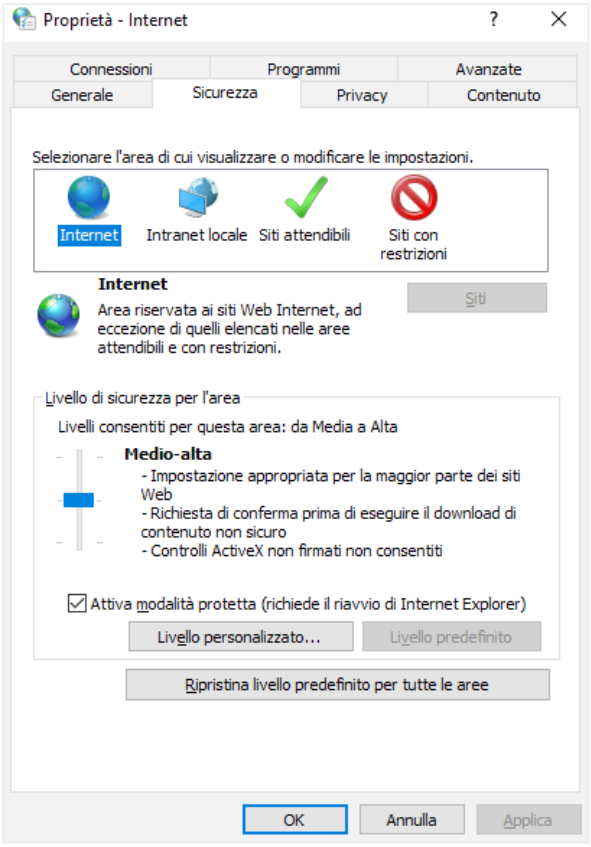
In italiano, questi script si definiscono *codici attivi*. I più diffusi sono *JavaScript* (e altri similari, come *VBScript, ECMAScript* e *Jscript*), i *Controlli ActiveX* e *Applet Java*.

Il lato negativo della cosa è che i *codici attivi*, pur non essendo affatto pericolosi in sé, sono spesso usati dai malintenzionati per eseguire codici *malevoli* sul computer dell'utente.

Il fatto è che molti siti sono cosi legati alle opzioni attivate da script che, qualora fossero disattivati dall'utente, molti servizi non potrebbero essere resi; ne consegue che la disattivazione completa non è consigliabile e può perfino risultare dannosa.

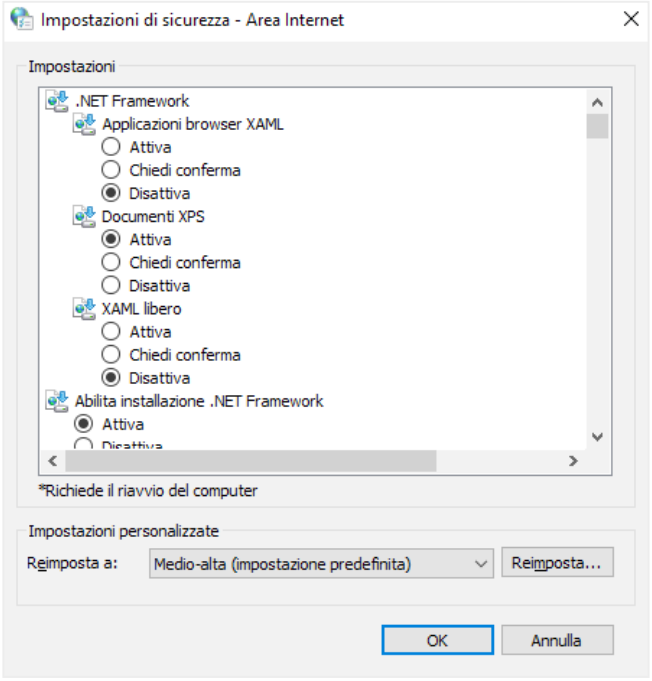
Impariamo, però, a controllarli: tutti i browser consentono di fare verifiche circa il funzionamento degli script.

1. Digita *Opzioni Internet* in Cortana e clicca su *Invio*. Si aprirà la finestra di dialogo *Proprietà-Internet*.
2. Clicca sulla scheda *Sicurezza*.



4.7 | Finestra di dialogo *Proprietà - Internet*

3. Nell'area *Livello di sicurezza per l'area,* clicca su *Livello personalizzato…* Si apre la finestra di dialogo *Impostazioni di sicurezza - Area Internet*.



4.8 | Finestra di dialogo *Impostazioni di sicurezza*

4. Visualizza tutte le opzioni di sicurezza, comprese quelle relative agli *script*. Scorri l'elenco e gestisci ogni script; puoi attivarne l'esecuzione, disattivarla o chiedere, ogni volta che serve, la conferma all'attivazione, mentre navighi.

Per operare scientemente, dovresti conoscere il funzionamento di ognuno degli script in elenco; se il tema di appassiona, sarebbe un buon esercizio fare apposite ricerche online.
Diversamente, potresti impostare il livello di sicurezza tra quelli preimpostati: *Alta*, *Medio-alta* (preimpostata) e *Media*.

4.1.5 I cookie

Ce ne sono di due tipi:

- I *cookies di sessione* memorizzano le informazioni soltanto fino a quando utilizzi il browser; quindi, quando lo chiudi, le informazioni sono automaticamente cancellate.
- I *cookies persistenti* sono immagazzinati sul tuo PC in modo da potere mantenere le vostre preferenze personali.

Anche della gestione dei cookie parliamo nel modulo dedicato alla navigazione in rete. In questa sede, sottoliniamo che le funzionalità di quelli persistenti pongono le stesse questioni di sicurezza viste per gli *script*.

È grazie a questi *cookie*, ad esempio, che il tuo indirizzo email appare automaticamente quando apri il tuo *account* di posta elettronica: se altre persone utilizzano il tuo PC, vedranno facilmente dati di questo tipo. Anche in questo caso, è consigliabile eliminarli o limitarli.

4.2 Gli strumenti di Google Chrome

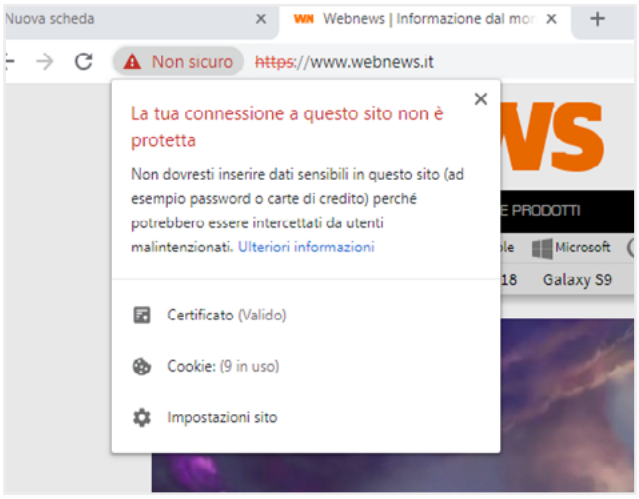
Oltre agli strumenti di protezione generici della tua privacy visti finora, ce ne sono altri messi a punto di ogni specifico browser. Vediamo quelli messi a punto da Google Chrome.

Il gruppo afferma di aver riconosciuto, fino a oggi, oltre 3,5 milioni di dollari alla community di ricercatori indipendenti, per compensare i loro sforzi nell'individuare e segnalare bug o vulnerabilità all'interno del codice di Google, così da poterle risolvere nel minor tempo possibile, mediante il rilascio di aggiornamenti.

4.2.1 Icone relative al protocollo SSL (Secure Socket Layer)

Quando ti connetti a un sito, Google Chrome ti mostra i dettagli relativi alla connessione e ti avvisa quando non è possibile stabilirne una totalmente protetta, tramite apposite icone posi-

zionate a sinistra dell'URL. Seleziona l'icona per visualizzare le informazioni dettagliate relative al sito su cui stai navigando.



4.9 | Icona nella URL

In sostanza, queste icone ti consentono di conoscere il livello di sicurezza di un sito, permettendoti di sapere se ha un *certificato di sicurezza*, se il certificato è ritenuto attendibile da Chrome e se quest'ultimo ha una connessione privata con il sito.

Cos'è un certificato di sicurezza?

Quando visiti un sito che utilizza HTTPS (il protocollo che garantisce la sicurezza della connessione), il server del sito web usa un certificato per dimostrare l'identità del sito ai browser come Chrome. Il punto è che chiunque può creare un certificato e dichiarare di essere un qualunque sito web. Per contribuire alla tua sicurezza, Chrome richiede ai siti web di utilizzare certificati di *organizzazioni terze attendibili* che rilasciano questi certificati in maniera professionale.

Impariamo a riconoscere le icone.

	Livello di sicurezza	Informativa
	Sito sicuro	Le informazioni inviate o ricevute tramite il sito saranno private. Anche se vedi questa icona, presta sempre attenzione quando condividi informazioni private. Controlla l'indirizzo nella barra degli indirizzi per verificare che si tratti del sito che desideri visitare.
	Sito non sicuro	Il sito non utilizza una connessione privata. Qualcuno potrebbe riuscire a visualizzare o modificare le informazioni inviate o ricevute tramite il sito. Potrebbe essere visualizzato un messaggio *Accesso non sicuro* o *Pagamento non sicuro*. Ti invitiamo a non inserire dati sensibili quali password o carte di credito.
	Non sicuro o pericoloso	Procedi con cautela. Sono presenti seri problemi con la privacy della connessione a questo sito. Qualcuno potrebbe riuscire a visualizzare le informazioni inviate o ricevute tramite il sito. Se il pericolo è alto, potresti verificare un avviso; ne parleremo tra breve.

4.2.2 Avvisi per siti non sicuri

Se ti trovi su un sito con contenuti pericolosi o ingannevoli, Chrome ti mostrerà un avviso in cui c'è scritto che ti trovi su un sito di phishing o malware. Il rilevamento è attivo per impostazione predefinita. Se visualizzi uno dei messaggi elencati di seguito, ti consigliamo di lasciare subito il sito:

	Avviso	Descrizione
1	Il sito che stai per visitare contiene malware	Il sito che vuoi visitare potrebbe cercare di installare sul computer software dannoso, chiamato *malware*.
2	Sito ingannevole in vista	Il sito che vuoi visitare potrebbe essere un sito di *phishing*.
3	Il sito che stai per visitare contiene programmi dannosi	Il sito che vuoi visitare potrebbe tentare di ingannarti inducendoti a installare programmi che causano problemi durante la navigazione online.
4	Questa pagina sta tentando di caricare script da fonti non autenticate	Il sito che stai visitando non è sicuro.

Ricordi in cosa consiste un attacco di *phishing*?
Si verifica quando qualcuno assume un'altra identità per indurti a condividere informazioni personali o confidenziali, generalmente tramite un sito web fasullo.
Il malware, invece, è un software che viene installato sul computer spesso a tua insaputa con lo scopo di danneggiare il computer o rubare informazioni.

Sii prudente quando scarichi contenuti. Alcuni siti cercano di ingannarti inducendoti a scaricare programmi software dannosi che ti vengono proposti come soluzione a un presunto virus rilevato. Fai attenzione a non scaricare programmi di questo tipo.

Google dichiara che gli utenti Chrome visualizzano in media 250 milioni di volte ogni mese un avviso dei tipi elencati.

È possibile disattivare questa funzione ma, considerato che è davvero consigliabile utilizzarla sempre, non ti diremo che si fa.

4.2.3 Sandboxing

Questo strumento aggiunge un ulteriore livello di sicurezza, proteggendo da pagine web dannose che tentano di installare programmi sul computer, monitorare le tue attività sul Web o carpire informazioni personali dal disco rigido.

4.2.4 Aggiornamenti automatici

Per fare in modo che gli utenti siano sempre protetti, Google Chrome controlla periodicamente la disponibilità di aggiornamenti di protezione.

Questo controllo garantisce l'aggiornamento automatico della tua versione di Chrome con le ultime funzioni e correzioni di sicurezza, senza che tu debba far nulla.

4.2.5 Google Smart Lock

Se hai un account Google, puoi utilizzare questa funzione per sincronizzare i tuoi dispositivi (PC, smartphone e tablet che utilizzino Android) e, quindi, accedere a siti e App a cui sei registrato, senza dover ogni volta inserire la password.

Per scoprire come attivare la funzione, ti rinviamo alla guida online di Chrome.

4.2.6 La protezione della privacy

Molti browser ti consentono di controllare le tue informazioni private, aiutandoti a proteggere le informazioni che condividi online. Vediamo gli strumenti messi a disposizione in questo senso da Google Chrome.

Navigazione in incognito

Quando non vuoi che le tue visite dei siti web o i tuoi download vengano registrati nelle cronologie di navigazione e dei download, puoi utilizzare la modalità di navigazione in incognito.

Quando chiudi tutte le finestre di navigazione in incognito, i cookie creati vengono automaticamente eliminati.

Vai al modulo dedicato alla navigazione in rete per vedere come si imposta e si gestisce la navigazione in incognito.

Preferenze per la privacy

Dal menu puoi gestire le impostazioni relative alla privacy.

Si tratta, per lo più, di strumenti che ti assicurano una migliore navigazione ma che, nel contempo, possono esporti a rischi; per questo sono quasi tutte attive per impostazione predefinita. Puoi disattivarli.

Clicca sul pulsante *Personalizza e controlla Google Chrome* ⋮ in alto a destra > *Impostazioni* > *Avanzate* e configura le opzioni come desideri.

Per ogni approfondimento, ti rimandiamo alla guida online di Google Chrome.

4.3 Strumenti di filtraggio dei contenuti

Un aspetto importante della sicurezza è quello relativo alla *protezione* degli utenti che navigano in rete. I browser più evoluti mettono a disposizione strumenti che consentono di filtrare determinati contenuti tra quelli ricavabili da una ricerca.

Anche in questo caso, approfondiamo l'analisi di Google Chrome.

4.3.1 Come gestire SafeSearch di Google Chrome

SafeSearch può esserti utile per impedire la visualizzazione di immagini esplicite o inappropriate nei risultati della ricerca di Google. Il filtro SafeSearch non è preciso al 100% ma consente comunque di evitare la maggior parte dei contenuti violenti e per adulti.

È molto utile se il PC è utilizzato da minori.

1. Visita la pagina Impostazioni di ricerca di Google.
2. Nella sezione *Filtri SafeSearch*, seleziona o deseleziona la casella *Attiva SafeSearch*.
3. Clicca su *Salva*, in fondo alla pagina.

Per utilizzare questo servizio e anche quello indicato nel paragrafo successivo, devi avere un account Google.

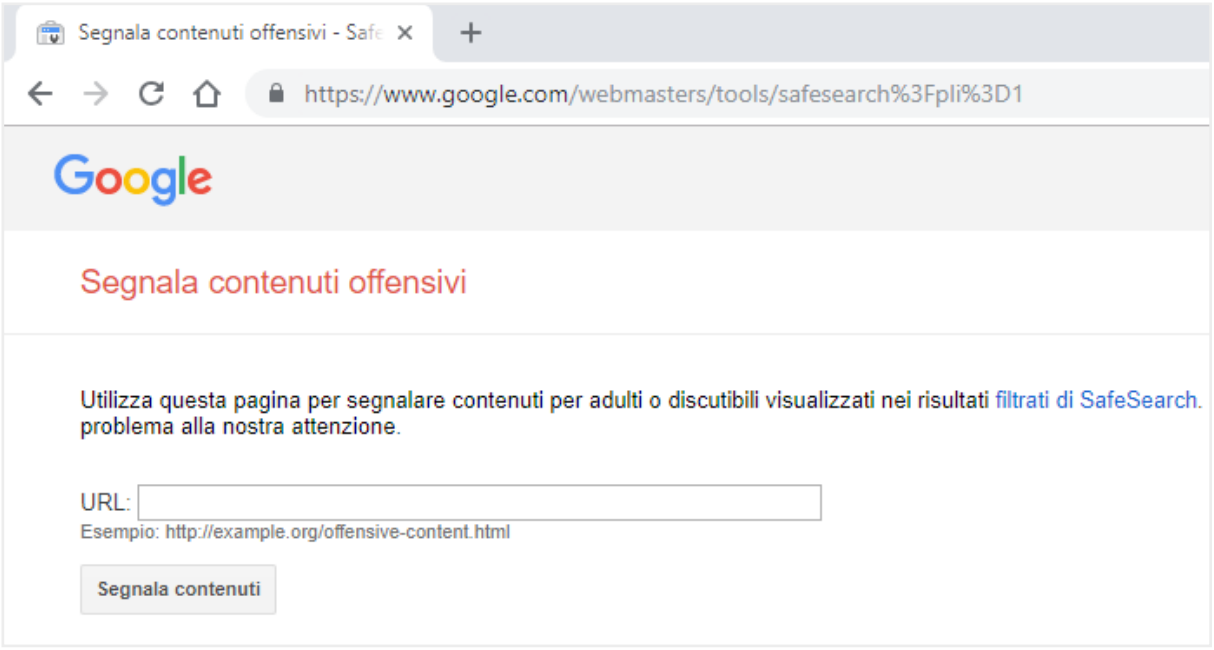
Per impedire ad altri di modificare la tua impostazione, selezione *Blocca SafeSearch*. Se imposti il blocco, Google utilizza un cookie per impedirne la rimozione da parte di chiunque non acceda con l'account Google che l'ha impostato.

4.3.2 Segnalazione di contenuti inappropriati

Se continui a visualizzare immagini esplicite anche dopo l'attivazione del filtro, puoi segnalare i siti che riportano queste immagini a Google che provvederà a migliorare il servizio.

Segnalare siti inappropriati

Clicca qui per accedere alla sezione di Google dedicata e incolla l'URL del sito da segnalare nella barra che visualizzi.



4.10 | Come segnalare siti con contenuti inappropriati

Segnalare immagini inappropriate

Se, dopo aver cercato nelle Immagini di Google, intendi segnalarne una, clicca sull'immagine e poi su Invia feedback, in basso a destra.

4.11 | Come segnalare immagini inappropriati

4.3.3 Il Centro per la sicurezza online di Google

Quelli visti finora sono solo alcuni degli strumenti che, nel tempo, Google ha prodotto e aggiorna per la sicurezza della nostra navigazione.

Se vuoi scoprirli tutti, ti invitiamo a visitare il Centro per la sicurezza online, un sito web che Google dedica interamente a questo argomento.

Se hai un account Google, è un'ottima guida per gestire tutte le opzioni di sicurezza su:

- Google Chrome,
- Google Play,
- Ricerche,
- Google+,
- Youtube,
- Blogger,
- Android.

4.3.4 Il Safety Family di Microsoft

Anche Microsoft lavora molto per rendere sicura la navigazione e filtrare i contenuti di Internet. Se in casa ci sono bambini o, comunque, utenti per cui si vuole controllare e gestire l'accesso a Internet, un amministratore può attivare diversi account, uno per ogni utente e settare diverse opzioni di navigazione e di utilizzo per ciascuno.

In questo modo, l'amministratore:

- sceglie i giochi, i programmi e i siti Web accessibili in base al contenuto e creando una *white list* per i propri figli;
- blocca la visualizzazione di video, immagini e link non adatti ai minori sui principali motori di ricerca;
- definisce le fasce orarie di utilizzo del PC;
- limitare la visualizzazione delle App di Windows Store;

Creati gli account, ogni utente accede separatamente al proprio profilo e, quindi, al proprio desktop.

Ogni settimana Windows 10 invia una mail all'account dell'amministratore, dettagliando il riepilogo di tutte le attività on line (siti visitati, tempo trascorso sul PC, parole ricercate sui motori di ricerca e così via) degli altri account.

Anche Microsoft dedica al tema un sito web.

4.3.5 Homeguard Activity Monitor e altri programma specializzati per il filtraggio dei contenuti

Oltre agli strumenti gratuiti messi a disposizione dai colossi del web, ci sono molte software house che, considerata la delicatezza del tema, producono software specifici per la sicurezza soprattutto degli internauti più giovani.

Homeguard Activity Monitor è uno di questi. Costa 40 dollari ed è caricabile direttamente dal sito della casa produttrice (veridium.net/).

Vediamo tutte le opzioni che mette a disposizione per comprendere cosa offre in più rispetto agli strumenti visti finora:

- impostazione dei filtri alla navigazione,
- blocco di siti con contenuto non conveniente,
- registrazione delle password utilizzate dagli altri utilizzatori del PC per accedere a determinati siti internet,
- blocco di determinati programmi installati sul PC,
- controllo delle chat,
- controllo delle e-mail ricevute dagli altri utilizzatori del PC,
- cattura e salvataggio di screenshot scattati ogni 30 minuti, ad esempio,
- controllo dei nuovi file caricati o salvati sul PC,
- limitazione degli orari di accesso a Internet.

Se sei interessato al tema, ti consigliamo di aprire questo link per conoscere alcuni dei migliori software di filtraggio gratuiti in circolazione, come K9 Web Protection, Qustodio Free, Social-Shield e così via.

5. SICUREZZA NELLE COMUNICAZIONI ONLINE

Considerato il largo uso che facciamo di e-mail, social network e messaggistica istantanea, è opportuno comprendere quali siano i rischi che ne derivano, dal punto di vista della sicurezza.

5.1 La vulnerabilità della posta elettronica

Benché la maggior parte degli utenti si connetta ai propri server di posta in maniera sicura (SSL), è possibile che estranei male intenzionati riescano a intercettare, leggere e alterare un messaggio durante il percorso che fa dal mittente al destinatario.

Possiamo distinguere le minacce in due gruppi principali:

- Infiltrazioni *malware*: gli allegati sono lo strumento più utilizzato per diffonderli.
- Posta indesiderata: considerati i costi minimi, la e-mail è molto utilizzata da chiunque voglia far conoscere o vendere qualcosa; è molto facile, quindi, che giornalmente, tu riceva messaggi da persone o aziende che non conosci e a cui non hai mai dato il tuo indirizzo né l'autorizzazione a inviarti comunicazioni.

5.1.1 La cifratura come argine alle infiltrazioni malware

Per tenere sicuri i nostri messaggi di posta possiamo cifrarli; possiamo, cioè, utilizzare programmi che ci consentono di crittografarli in modo che non siano più leggibili o alterabili da eventuali intrusi. Alcuni di questi programmi sono online (webmail), altri sono da installare sul PC.

Vediamo alcuni esempi.

Virtru consente di crittografare e-mail inviate con numerosi programmi webmail, tra cui Gmail, Outlook, Yahoo. Dopo aver installato l'apposita estensione per Chrome, Firefox o Internet Explorer, ogni messaggio inviato sarà crittografato automaticamente.

Si può anche installare come plugin per Microsoft Outlook.

ProtonMail è uno dei servizi di cifratura per e-mail più popolari al mondo. Se intendi utilizzarlo, crea un nuovo indirizzo e-mail su questo sito: le e-mail inviate tra utenti che hanno un indirizzo Protonmail vengono crittografate e decrittografate automaticamente.

Nel caso invece la mail venisse inviata verso un indirizzo di posta normale, allora si può usare una domanda segreta a cui il destinatario deve rispondere per poter leggere il messaggio.

Sbwave Enkryptor è un servizio gratuito per crittografare messaggi di testo da spedire via e-mail.

Per leggere il messaggio, il destinatario deve avere una password.

Per utilizzarlo, non devi installare software o iscriverti al sito e non vedrai annunci pubblicitari.

Vai sul sito di Lockbin, premi sul pulsante verde Start e usa l'interfaccia di composizione del

messaggio con una password di protezione che sarà indispensabile per poterlo leggere.

Il destinatario della mail criptata riceve una e-mail da Lockbin con un link da cliccare che porta alla pagina protetta dove deve scrivere la password.

Encipher.it è un sistema di protezione semplice da usare che garantisce comunque un crittografia *Advanced Encryption Standard* (AES).

Si tratta di un bookmarklet, ossia di un link da aggiungere alla barra dei preferiti del browser.

Ogni volta che si scrive un messaggio, su Gmail, su Facebook o su altri servizi web, dopo averlo scritto, basta premere il link di Encipher salvato nei preferiti per attivare il sistema di protezione.

Chi riceve il messaggio potrà leggerlo solo conoscendo la password e, ovviamente, deve avere anche lui il bookmarklet di Encipher.it.

Secure Gmail è l'estensione gratuita che ti consente di crittografare e inviare mail usando Gmail.

5.1.2 Firma digitale e crittografia

La firma digitale è un altro strumento per rispondere in maniera efficace alle minacce nascoste nel web. Vediamo come funziona, per comprenderne le differenze rispetto alla cifratura.

- Quando si appone la firma digitale a un messaggio, al suo interno vengono incorporate le informazioni che certificano l'identità del mittente;
- Quando un messaggio viene criptato, appare *scritto in codice* e può essere letto soltanto da un destinatario che sia in possesso della chiave adatta a decriptarlo.

La firma digitale garantisce che il messaggio inviato sia stato effettivamente spedito da un mittente certificato; la criptazione fornisce la certezza che il messaggio non sia stato letto o alterato durante la sua trasmissione.

5.1.3 Le caratteristiche del phishing

Sapendo che moltissimi malware si diffondono automaticamente nel nostro PC nel momento stesso in cui scarichiamo un allegato infetto, qui ci concentriamo sul phishing per imparare a riconoscere e a gestire il malware più utilizzato per carpire dati in rete in modo fraudolento.

Abbiamo già visto come funziona: criminali cibernetici inviano e-mail apparentemente ufficiali di banche, fornitori di servizi di pagamento e negozi online, in cui si chiede all'utente di inserire dati, o cliccare su link che rimandano a pagine di login false.

L'obiettivo di questo tipo di attacchi è quello di acquisire nomi utente, password e PIN, per fare prenotazioni o acquisti a nome dell'utente derubato che, purtroppo, si accorge della cosa solo quando vede il suo estratto conto!

Come riconoscere e-mail fraudolente

La regola principale per riconoscere una truffa on-line è quella di drizzare le antenne!

Con un po' di attenzione, infatti, puoi rilevare abbastanza facilmente un tentativo di phishing. Vediamo gli elementi da tenere d'occhio.

- Se ricevi una mail da una banca, un ente pubblico o una grossa azienda, verifica se sei entrato già in contatto o hai fornito il tuo indirizzo alla persona o all'ente che compare come *mittente*.

Visualizza l'intero indirizzo e confrontalo con i messaggi che potresti già aver ricevuto dall'ente. Se non dovessero coincidere, allora è probabile che si tratti di una frode.

- Di solito enti e aziende si rivolgono ai loro clienti chiamandoli per nome; i truffatori spesso non hanno questo dato: se un messaggio della tua banca comincia con *Gentili Signori e Signore* o altre forme generiche, ti conviene diffidare.
- Se un messaggio di posta elettronica è pieno di *errori grammaticali*, è molto probabile che si tratta di una truffa: errori di ortografia e informazioni contorte sono un chiaro indizio delle intenzioni fraudolente di quella e-mail, scritta probabilmente in un'altra lingua e poi tradotta da traduttori automatici.

Lo stesso vale spesso per testi contenenti parole non accentate o lettere di altri alfabeti.

- Se un messaggio contiene un link, ti conviene verificarlo, prima di cliccarci su. Posiziona il mouse sul link e controlla l'indirizzo Internet mostrato in basso a sinistra nella finestra del browser.

Controlla che:

- l'URL coincida con quello che ti aspetti, visto il contento e il mittente;
- siano presenti protocolli HTTP di sicurezza per la trasmissione di dati.

Se hai dubbi, non cliccare sul link e non inserire manualmente l'URL nel tuo browser.

- Nessun negozio online chiede ai propri clienti di trasmettere dati personali tramite e-mail. Se in un messaggio ti trovi davanti a un form da compilare, puoi star certo che si tratta di un tentativo di *phishing*. Stesso discorso vale per i codici PIN.

- Se una mail 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, chiama l'assistenza clienti del mittente.

Cosa fare contro i tentativi di phishing

Se ricevi un'e-mail che sembra un tentativo di *phishing*, spostala nella cartella *Spam* della tua casella di posta e blocca il mittente. In questo modo bloccherai altri eventuali attacchi provenienti dallo stesso mittente. Vedremo tra breve come si fa.

Puoi, inoltre, contattare l'azienda o la persona per cui si sta spacciando chi vi ha inviato l'e-mail. La maggior parte delle aziende mette a disposizione diverse possibilità di contatto, come per esempio moduli da compilare, con cui è possibile segnalare un tentativo di phishing.

5.1.4 La posta indesiderata

Lo spam, cui abbiamo appena adesso accennato, è un classico esempio di posta indesiderata.

L'origine del termine è molto curiosa: sembra sia stato preso da una delle cervellotiche scenette tipiche del *Flying Circus* dei *Monty Python*, un gruppo di comici davvero *British*, in voga negli anni settanta: due clienti chiedono cosa ci sia per colazione e l'originale cameriera fa un elenco di pietanze in cui c'è sempre *spam* (si tratta di una marca di carne in scatola); dice così tante volte *spam* che non si capisce nulla del menù!

Parlando di posta elettronica, possiamo definire lo spam come un disturbo alla nostra comunicazione online, arrecato da terzi mediante l'invio di messaggi non richiesti.

Lo *spammer* è colui che invia, tutte assieme, tantissime email a scopo pubblicitario o per fare phishing, senza alcun consenso da parte del destinatario, anche per conto di terzi: ci sono aziende che fanno questo per lavoro!

Quante sono le e-mail spam?

Non è così semplice fare delle stime, peraltro in continuo aumento. Per darti un'idea, ti diamo comunque dei dati:

- più di 2 miliardi di persone scrivono 144 miliardi di email al giono. Il 70% sono spam!
- Il 50% di spam è inviato da o per conto di case farmaceutiche.
- Il 16% è relativo a prodotti sessuali.
- Il 15% tratta articoli da regalo.
- La restante percentuale è divisa tra mutui e prestiti e altri prodotti commerciali.

Quello che è importante comprendere è che non stiamo parlando solo di un fastidio più o meno sopportabile ma di un danno economico non di poco conto. Pensa, infatti a:

- il tempo perso dai destinatari per scaricare, verificare e cancellare il messaggio,
- i costi sostenuti dagli ISP per la gestione della banda e dai destinatari che pagano la bolletta per scaricare comunicazioni inutili, quando non dannose.

Cosa fare per non essere spammato

- *Non pubblicare il tuo indirizzo e-mail in pagine web*. Un esempio pratico? Se lavori in un'azienda e tu e i tuoi colleghi avete tutti una mail personale, conviene pubblicare solo mail generiche (*info@azienda.it*) piuttosto che tutte quelle effettivamente funzionanti. Se gestisci un blog o hai un profilo su un *social*, ti consigliamo di non pubblicare il tuo indirizzo email. Se proprio devi farlo, inseriscilo come *immagine*: i *software* degli *spammer* alla ricerca di indirizzi non lo vedranno, le persone interessate a scriverti si.
- Anche se partecipi a *forum*, *chat o newsproup*, non è necessario indicare il tuo indirizzo, a meno che tu non voglia essere contattato in privato dagli altri utenti.
- Uno dei trucchi più utilizzati dagli *spammer* per indurti a rispondere e verificare che, in effetti, il tuo indirizzo sia un valido bersaglio, è quello di inserire nei messaggi false opzioni di cancellazioni (del tipo *Se non vuoi ricevere altre mail da noi, clicca qui*). *Non rispondere mai, non serve protestare*.
- *Non inserire l'indirizzo e-mail nel browser*. Abbiamo visto che i browser ti consentono di memorizzare i tuoi dati personali, in modo che tu non debba inserirli ogni volta che hai bisogno di creare un account o fare acquisti online. La funzione è molto *comoda* ma devi sapere che questo è uno degli strumenti più attaccabili da chi è alla ricerca di indirizzi da bersagliare.
- Ricordati di *usare e fare usare sempre la copia carbone nascosta*. Quando devi inviare lo stesso messaggio a più persone, scegli sempre l'opzione di invio che ti consente di non far vedere tutti gli indirizzi dei destinatari.
- Quando usi un servizio online (fai un acquisto, ad esempio) *leggi l'informativa sulla privacy* per verificare che non sia prevista la divulgazione del tuo indirizzo ad altre aziende partner: spesso puoi scegliere se lasciare questa libertà o meno al gestore del sito.

5.1.5 Come gestire in sicurezza una casella di posta su Gmail

Mettiamo in pratica quello che abbiamo imparato finora, utilizzando un account di Gmail, la casella di posta elettronica di Google, una delle più usate al mondo.

Per cominciare, ripetiamo le poche e semplici norme sulla scelta della *password* (più è complessa più è difficile che altri se ne approprino o possano scoprirla):

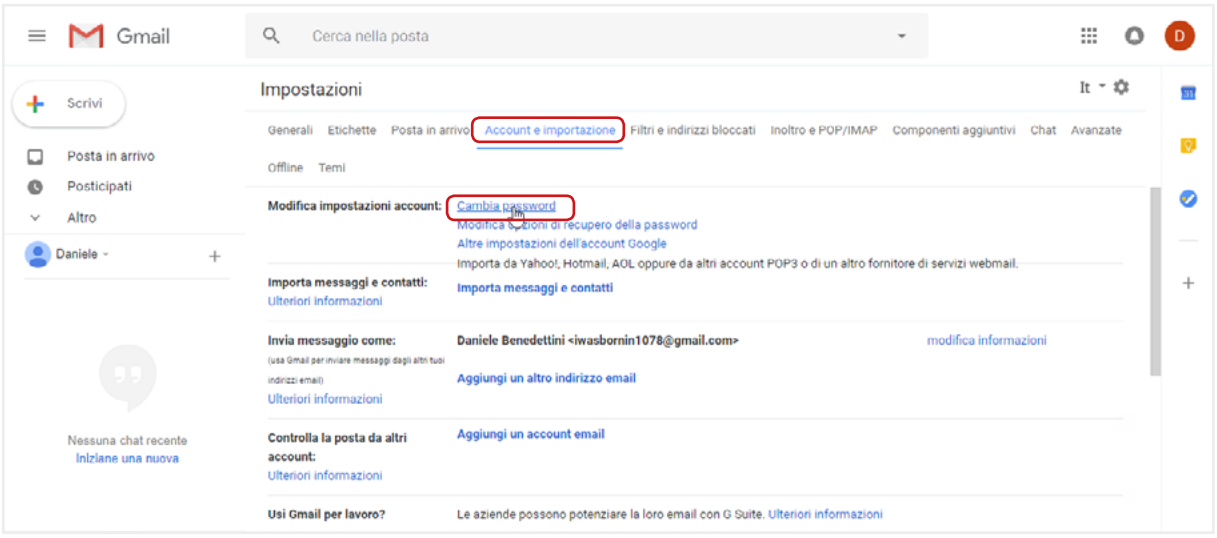
- Deve essere composta da almeno 6/8 caratteri,
- Deve contenere numeri, lettere (minuscole e maiuscole) e simboli (! ? _ -)

- Non deve mai essere lasciata in giro (come ad esempio su un post-it o su un foglietto).
- Non devi mai inviarla tramite e-mail e chat.

Nella figura che segue, vediamo il login tramite cui creare un account Gmail e poi accedere alla casella di posta elettronica.

Cambia spesso la tua password: è il modo migliore per tenere al sicuro il tuo account.

Per cambiare la tua password, clicca in alto a destra su , poi su *Impostazioni*; seleziona la scheda *Account e Importazione* e scegli *Cambia password*.



5.1 | Come cambiare la password in Gmail

1. Si aprirà una scheda nella finestra del tuo browser.
2. Conferma la tua identità e clicca su *Avanti*.
3. Inserisci due volte la nuova password.
4. Clicca su *Cambia password*.

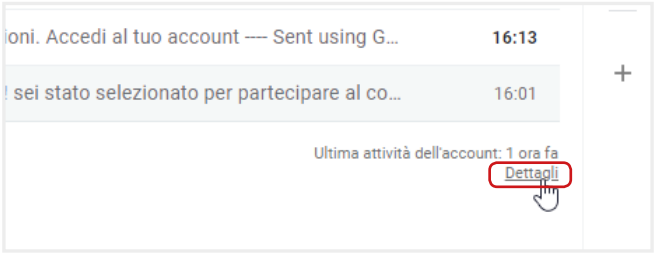
Strumenti per la sicurezza dell'account Gmail

Gmail mette a disposizione diverse tipologie di strumenti per la sicurezza del tuo account:

- quelli passivi ti permettono di monitorare e segnalare azioni altrui;
- quelli attivi servono a prevenire le azioni altrui; puoi impostarli tu stesso. Il più importante è il filtro anti spam; lo vedremo nella prossima sezione.

Puoi monitorare le tue ultime attività verificando, ad esempio, che non ci siano stati eventuali *accessi non autorizzati* alla tua casella di posta.

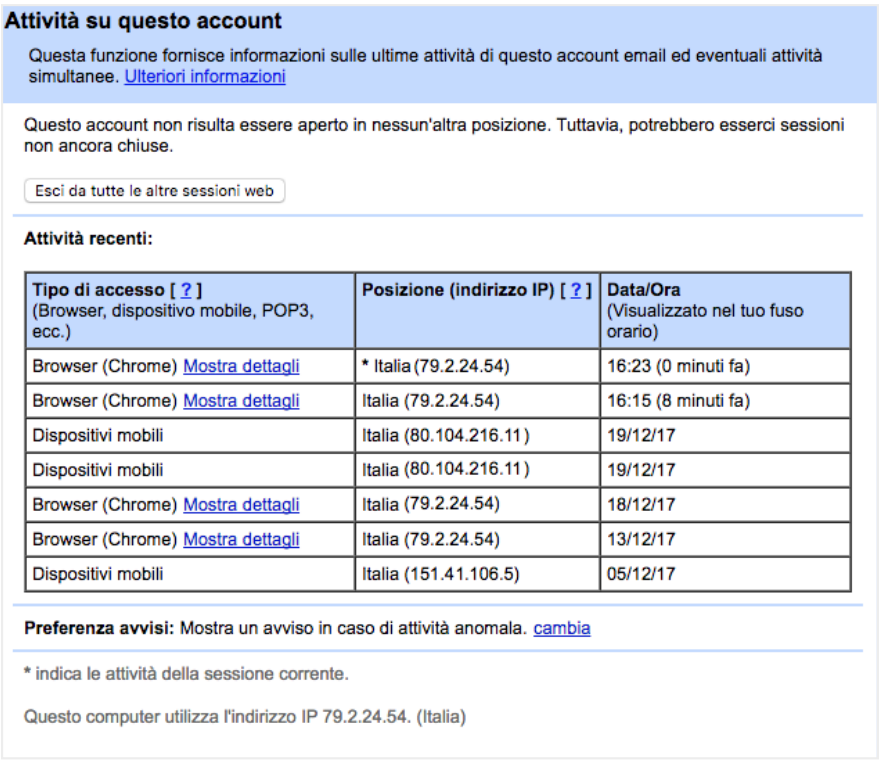
Vai su *Dettagli*, nella parte inferiore dell'interfaccia di Gmail, come mostrato nella figura.



5.2 | Apri *Attività recenti* da *Dettagli*

Si apre una pagina con i seguenti dati, ordinati in colonna:

- *Tipo di accesso*, consente di controllare da dove è stato fatto l'accesso alla casella di posta (nell'esempio che segue, è facile notare che gli accessi sono stati fatti tutti dal browser Google Chrome; un utente avveduto che abbia sempre fatto accesso in questo modo, dovrebbe allarmarsi qualora risultasse da questo elenco un accesso da *smartphone* o da un altro browser!).
- *Posizione IP*, indica l'indirizzo univoco del PC utilizzato per accedere all'*account*. Anche in questo caso, vediamo che il PC è sempre lo stesso; se l'utente sa di non aver fatto accessi da altri PC eppure ci sono altri indirizzi IP, qualcosa non quadra!
- *Data e ora* di ogni accesso. Vale quanto appena detto.



Attività su questo account

Questa funzione fornisce informazioni sulle ultime attività di questo account email ed eventuali attività simultanee. Ulteriori informazioni

Questo account non risulta essere aperto in nessun'altra posizione. Tuttavia, potrebbero esserci sessioni non ancora chiuse.

Esci da tutte le altre sessioni web

Attività recenti:

Tipo di accesso [?] (Browser, dispositivo mobile, POP3, ecc.)	**Posizione (indirizzo IP) [?]**	**Data/Ora** (Visualizzato nel tuo fuso orario)
Browser (Chrome) Mostra dettagli	* Italia (79.2.24.54)	16:23 (0 minuti fa)
Browser (Chrome) Mostra dettagli	Italia (79.2.24.54)	16:15 (8 minuti fa)
Dispositivi mobili	Italia (80.104.216.11)	19/12/17
Dispositivi mobili	Italia (80.104.216.11)	19/12/17
Browser (Chrome) Mostra dettagli	Italia (79.2.24.54)	18/12/17
Browser (Chrome) Mostra dettagli	Italia (79.2.24.54)	13/12/17
Dispositivi mobili	Italia (151.41.106.5)	05/12/17

Preferenza avvisi: Mostra un avviso in caso di attività anomala. cambia

* indica le attività della sessione corrente.

Questo computer utilizza l'indirizzo IP 79.2.24.54. (Italia)

5.3 | Attività su questo account

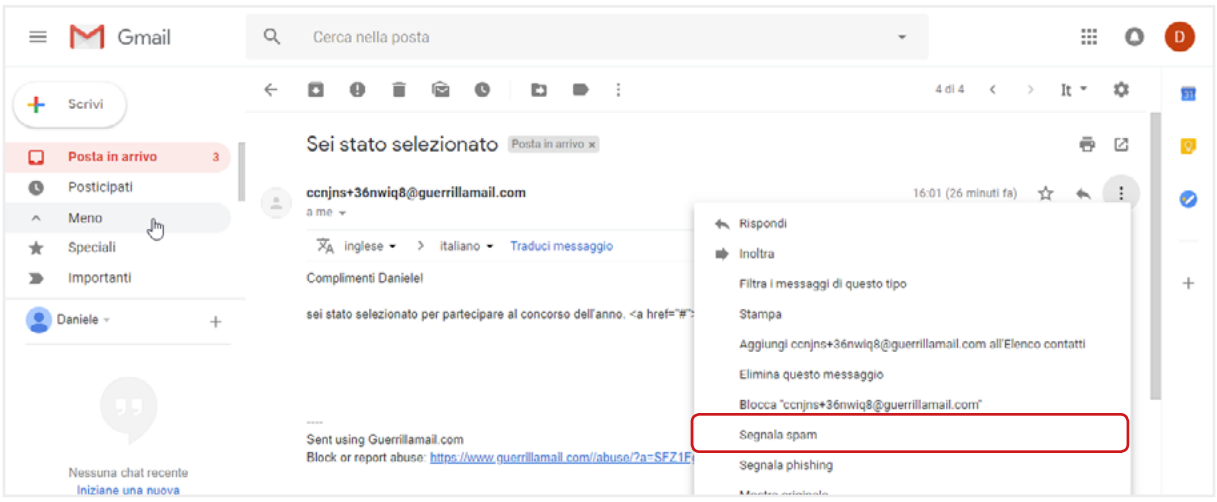
Controllando questa tabella, puoi verificare se sei vittima di un attacco *spoofing* o se qualcuno si è appropriato e ha utilizzato il tuo *account*.

Puoi, inoltre, segnalare:

- Un tentativo di *phishing* (messaggi che ti richiedono informazioni personali),
- Mail *spam* (con contenuto non desiderato o per cui non hai mai autorizzato la ricezione o, semplicemente, non desiderata).

In entrambi i casi:

1. Apri il messaggio che desideri segnalare.
2. Clicca sul pulsante *Altro*
3. Nel menu a tendina, clicca su *Segnala phishing* o *Segnala Spam*.



5.4 | Segnalazione di mail indesiderate

La mail segnalata come *spam*, viene spostata nell'apposita cartella.

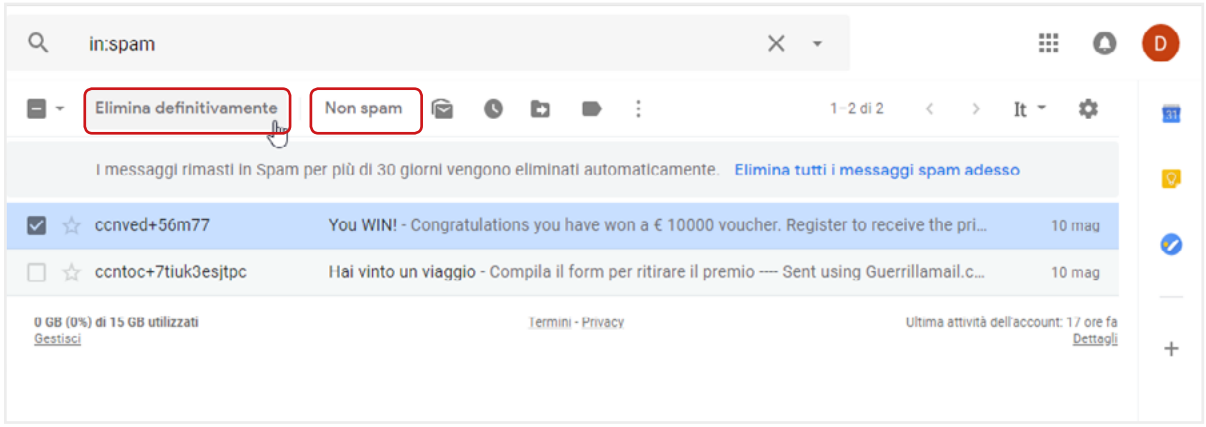
Per rimuovere definitivamente queste mail:

1. Fai clic su *Spam* nel menu a sinistra. Se la voce *Spam* non compare, clicca su *Altro*: il menu si espande mostrando tutte le opzioni.
2. Clicca su *Spam*.
3. Seleziona il o i messaggi che desideri eliminare e fai clic sul comando in alto *Elimina definitivamente*.

Segnala sempre i messaggi che non desideri ricevere. In questo modo, aiuterai Gmail a rendere più efficiente il sistema che tende a eliminare il problema dello *spam*.

In questa stessa pagina, puoi decidere di *salvare* un messaggio che Gmail o tu stesso hai precedentemente contrassegnato come *spam*.

Selezionalo e fai clic su *Non spam* nella parte superiore dell'interfaccia. Sarà automaticamente spostato nella *posta in arrivo*.



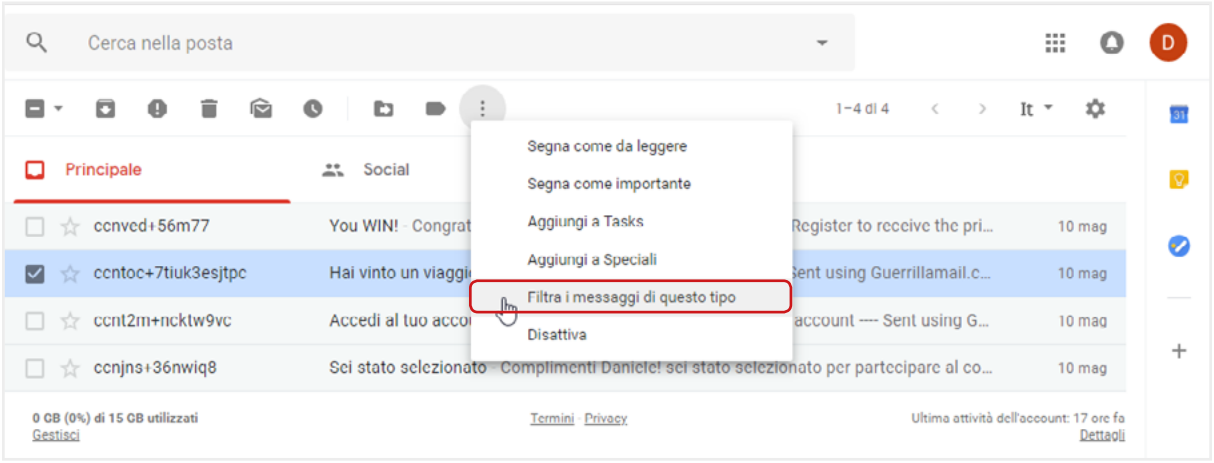
5.5 | La cartella *Spam* di Gmail

L' uso di un filtro antispam per le email

Impostare il *filtro antispam* è uno dei modi migliori per rendere sicuro il nostro account.

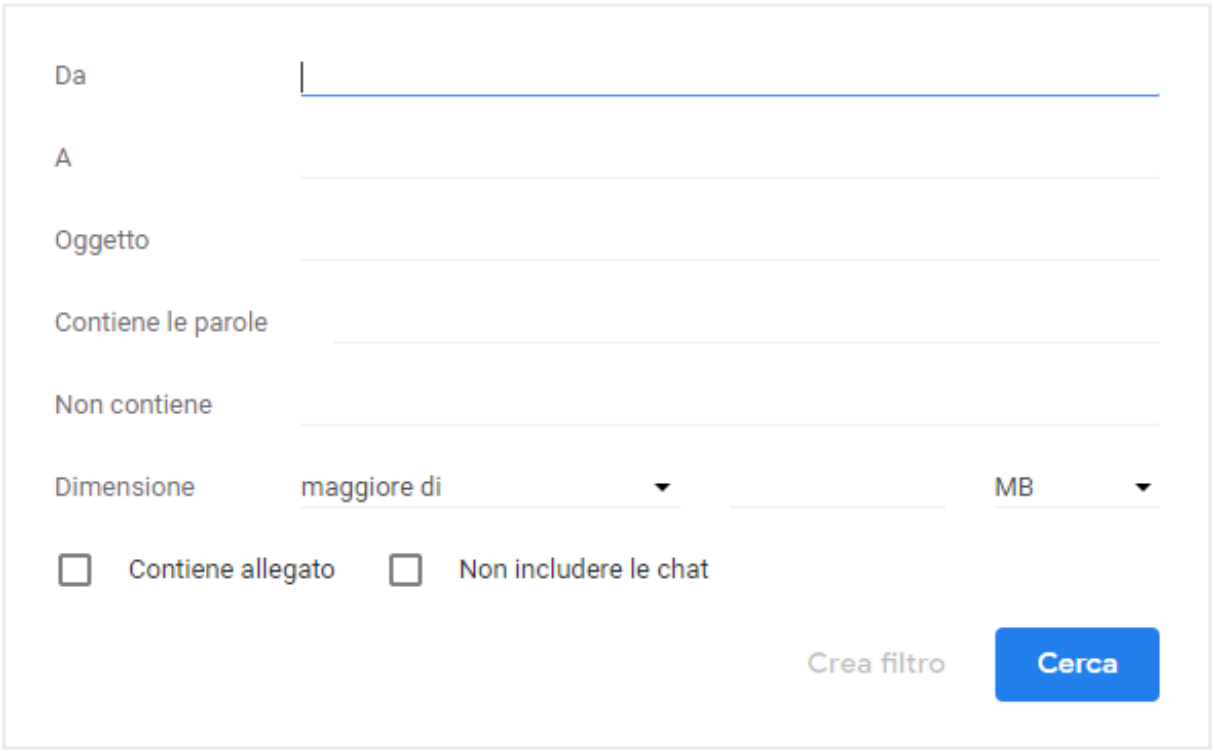
È molto semplice. Quando ricevi una mail indesiderata:

1. Selezionala.
2. Clicca sullo strumento *Altro* nella barra delle etichette.
3. Seleziona la voce *Filtra i messaggi di questo tipo*.



5.6 | Filtra i messaggi

4. Accedi a una finestra in cui devi riempire appositi campi che corrispondono ai criteri del tuo nuovo filtro.



5.7 | Attivazione dello spam

Puoi modificare o eliminare filtri esistenti.

1. Apri Gmail.
2. Fai clic sull'icona a forma di ingranaggio in alto a destra 
3. Seleziona *Impostazioni*.
4. Fai clic sulla scheda *Filtri e indirizzi bloccati*.
5. Scegli il filtro e clicca su
   - *Modifica*. Si apre la finestra che ti permette di cambiare i criteri. Finito l'aggiornamento, clicca su *Continua*.
   - *Elimina*. Si apre la finestra in cui confermare l'eliminazione del filtro.
6. Aggiorna le azioni e fai clic sul pulsante *Aggiorna filtro*.

Gli altri servizi di posta elettronica tengono in assoluto risalto il comando relativo allo spam (sempre nel menù principale delle funzioni disponibili) e all'organizzazione dei filtri che funzionano in maniera analoga a quanto visto qui.

Cura con attenzione la sicurezza della tua casella di posta elettronica: se sei oggetto di furto di identità, ad esempio, potresti essere costretto a eliminarla totalmente, perdendo tutti i file e le comunicazioni archiviate. Ovviamente, non potresti più utilizzare lo stesso indirizzo mail!

5.2 Come gestire gli strumenti di comunicazione online

Oltre all'*informatizzazione delle procedure*, ciò che maggiormente caratterizza l'ICT è la varietà e l'usabilità degli strumenti disponibili per comunicare online.

Questi strumenti hanno determinato un sostanziale cambiamento, a livello socio-culturale, del modo di conoscere e farsi conoscere, introducendo modalità che, pur se molto efficaci, lasciano aperte falle e quesiti su temi determinanti, come quelli che stiamo discutendo in questo modulo (privacy e sicurezza).

5.2.1 I possibili rischi alla sicurezza di blog e Social network

Usare i Social o un blog è davvero facile e intuitivo.

Il lato oscuro di questa praticità sta nel fatto che quasi mai ci soffermiamo sulle opzioni che ci consentirebbero di navigare con maggiore sicurezza, riducendo di molto i rischi cui siamo quotidianamente sottoposti.

Qualche dato (fonte digital4.biz)?

- Il 75% degli italiani pensa che le informazioni scambiate sul Web non siano di alcun interesse per i criminali.
- 1 utente su 10 parla di questioni molto private con estranei appena conosciuti sui Social.
- Il 15% fa circolare tranquillamente informazioni riservate.

- Il 12% inserisce i propri dati negli account online mentre è connesso a una rete Wi-Fi pubblica.
- Il 39% non chiude la sessione quando esce da un Social.
- Tantissimi utilizzano le stesse credenziali per accedere a diversi account.

Sono proprio questi cattivi comportamenti a favorire coloro che hanno, invece, molto interesse a reperire i nostri dati, sapendo come utilizzarli per finalità lucrative, spesso illegali.

È possibile che qualcuno abbia già acquisito i tuoi dati e/o le tue credenziali e le stia utilizzando, se:

- Ricevi messaggi dai Social, che ti chiedono di cambiare alcune impostazioni (ad esempio, la email, la foto o le impostazioni di privacy);
- Qualcuno dei tuoi contatti ti dice che ha ricevuto tuoi messaggi tramite mail e/o messaggistica e tu, invece, negli ultimi tempi, non ne hai inviate;
- Rilevi attività (come Mi Piace, Condividi, richieste di amicizia) che sembrano siano state avviate automaticamente;
- Ti accorgi che sul tuo PC o sul tuo smartphone ci sono giochi o applicazioni che tu non hai scaricato;
- Rilevi aggiornamenti di stato nei Social che tu non hai fatto.

In casi del genere, devi subito cambiare le password e, a seconda dei casi, rivolgerti ai fornitori dei servizi per richiedere informazioni o il blocco di eventuali azioni in corso.

Attivazione e gestione di account

Abbiamo visto come attivare, ad esempio, un account di Gmail; le stesse regole circa la creazione e la conservazione delle credenziali vale per ogni altro account tu voglia aprire.

Qui ti proponiamo di riflettere su un altro aspetto e, cioè, circa l'opportunità o meno di pubblicare e condividere determinate informazioni personali tramite i Social.

Da questo punto di vista, infatti, è importante sapere che ogni dato pubblicato può diventare oggetto, non solo di appropriazione indebita, ma anche di analisi e studio.

Sono molti, infatti, coloro che, a seconda dei casi, sono o possono essere interessati… a conoscerti meglio. Qualche esempio?

- Di solito, tra le condizioni che accetti (senza mai leggere!) quando ti iscrivi a un Social, c'è il consenso, rilasciato al gestore del servizio, di trasferire i tuoi dati a terzi per finalità statistiche o, molto più spesso, commerciali. Anche se tu decidessi di cancellare il tuo account, questi dati resterebbero, per il gestore e i terzi, disponibili e utilizzabili. In casi del genere, è certo che riceverai proposte commerciali che non hai mai richiesto, anche dopo che avrai eventualmente chiuso quell'account.
- I tuoi dati possono essere cercati e visionati, a tua insaputa, dall'azienda a cui hai mandato il curriculum, proponendoti come collaboratore. È molto probabile che vogliano farsi un'i-

dea su di te, ancor prima di un eventuale colloquio.

- Se è vero che ognuno di noi è libero di esprimere le proprie idee, anche politiche e/o religiose ed etiche, è altrettanto vero che anche i governi occidentali hanno cominciato ad acquisire dai Social 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 più, la conseguenza di esternazioni fatte e acquisite sui Social.

Ciò premesso, ti proponiamo alcuni consigli utili per utilizzare con maggiore sicurezza i blog e i Social.

La sicurezza nei blog

La metà dei blogger sono adolescenti che, nella maggior parte dei casi, indicano la propria età e rivelano il proprio indirizzo e altre informazioni di contatto.

La crescente competitività, inoltre, porta molti a fare di tutto per attrarre l'attenzione: capita spesso, quindi, che i ragazzi pubblichino materiale non adeguato (come, ad esempio, fotografie provocanti di se stessi o di amici).

Sarebbe opportuno che, assieme ai genitori, fossero stabilite regole condivise circa:

- il tempo concesso per restare connessi in Internet o anche solo per utilizzare il PC di casa o lo smartphone;
- la verificare del materiale che i ragazzi intendono pubblicare, prima che siano già online. Anche foto apparentemente innocue, ad esempio, possono causare problemi;
- controllo della piattaforma del blog: se c'è un'area privata protetta da password, è giusto che sia condivisa.

Questi suggerimenti, come quelli che seguono, non possono essere esaustivi ma sono un buon punto di partenza.

- Non fornire informazioni personali (come, ad esempio, cognome, informazioni di contatto, indirizzo di casa, numeri di telefono, indirizzo di posta elettronica, cognomi di amici o familiari, nomi di messaggistica istantanea, età o data di nascita).
- Non pubblicare immagini provocanti di se stessi o di altre persone e accertarsi che le immagini pubblicate non rivelino alcuna informazione personale.
- Riflettere sempre prima di pubblicare qualcosa, poiché il materiale pubblicato sul Web è permanente (aldilà del discusso diritto all'oblio). Chiunque, infatti, può stampare facilmente l'articolo di un blog o salvarlo per sempre sul suo computer.
- Utilizzare i siti di provider più conosciuti, in cui le note legali sono chiare e spiegate.
- Non entrare in competizione con altri blogger. È sempre preferibile avere un approccio positivo e mai mirato alla calunnia o all'attacco degli altri utenti o di persone e istituzioni pubbliche.

Vediamo più nello specifico alcuni consigli utili per chi utilizza un blog di Wordpress (uno dei più utilizzati).

- È necessario tenere sempre aggiornato il software. Quindi, appena riceviamo notifiche di nuovi aggiornamenti disponibili, procediamo subito. Si aggiornano l'istallazione di Wordpress, i plugin, i temi.
- È fondamentale utilizzare password appropriate.
- Bloccare lo spam, tramite plugin come Akismet.
- Eseguire periodicamente una scansione. Un utile plugin è Wp Security Scan.

La sicurezza nei Social network

Tutti i Social hanno ricche sezioni dedicate all'assistenza degli utenti.

Quella di Facebook, ad esempio (Centro assistenza), dedica molto spazio agli strumenti messi a disposizione per curare privacy e sicurezza.

Augurandoci che quello che abbiamo detto finora stia cominciando a stuzzicare il tuo interesse, ti diamo qualche dritta in proposito.

Tieni sempre presente che:

- Anche il tuo profilo, come quello di molti, è pubblico (visibile, cioè a tutti o quasi),
- Facebook modifica le impostazioni sulla privacy, rendendo pubbliche delle informazioni che prima erano visibili solo agli amici: è importante, quindi, prendere la buona abitudine di rivedere, di tanto in tanto, le impostazioni sulla privacy.

1. Impedisci ai tuoi amici di condividere le tue informazioni.
2. Rimuovi la tua faccia dai suggerimenti di tag.
3. Controlla i tag e decidi se approvare la foto (o video, o post); se non approvi, non verrà pubblicata sul tuo diario e non sarà visibile dai tuoi amici.
4. Restringi il pubblico per i vecchi post.
5. Imposta il livello di privacy che ritieni più appropriato per le informazioni che hai pubblicato sul tuo profilo.
6. Disattiva la ricerca pubblica per evitare che il tuo profilo compaia nei risultati dei mototi di ricerca (Google, Bing ecc.).

Sarebbe davvero un buon esercizio, adesso, connetterti al centro assistenza e mettere in pratica questi consigli, aggiornando il tuo profilo Facebook!

Facciamo un breve cenno anche alla gestione di sicurezza e privacy su Twitter.

Il punto di partenza è che, se le impostazioni dell'account non vengono modificate, tutti i tweet e i contenuti condivisi sono visibili a tutti, senza alcuna distinzione tra followers e no.

Se vuoi rendere privati i tuoi tweet, quindi, devi modificare le impostazioni.

Una volta fatto l'accesso:

1. Clicca sull'ingranaggio, in alto a destra.
2. Seleziona la *Impostazioni*.
3. Nella finestra che si apre, abilitiamo la casella *Privacy dei Tweet*.

Abilitata questa opzione, i tuoi tweet:

- saranno visualizzabili solo da chi decide di diventare tuo follower (da questo momento, ogni utente che richiede di diventarlo deve attendere la tua autorizzazione),
- non saranno visibili nella ricerca di Twitter e neanche in quella di Google,
- non potranno essere retweettati (nessuno, cioè, che non sia follower potrà rispondere).

Anche in questo caso, una volta registratoti, potrai accedere a una sezione dedicata al tema.

Consigli utili

Aldilà delle opzioni che decidi di impostare, ricorda sempre di usare questi strumenti in maniera equilibrata, non facendoti prendere dalle dinamiche di gruppo.

- Se, ad esempio, una tua amica pubblica il suo numero di telefono o foto in cui sono raffigurate in pose non proprio eleganti, non devi sentirti obbligata a farlo anche tu! Se la cerchia dei tuoi amici ti fa dei problemi per cose di questo genere… cambia amici!
- Fai attenzione a pubblicare informazioni personali (foto della tua casa, della tua azienda o della tua scuola, il tuo indirizzo, la data di nascita e il nome per intero): sono informazioni utilissime per chi intende adescare!
- Scegli un username che non contenga alcun dato personale (come Giovanni Roma o Lucia Firenze) e non usate mai come password informazioni personali come il codice fiscale o la data di nascita e così via.
- È buona norma aprire un account email separato, che non contenga il tuo nome per intero, da utilizzare per inviare e ricevere comunicazioni dai siti Web. In questo modo, se vorrai interrompere la connessione con quel sito, ti basta smettere di usare quell'account.
- Non scrivere o pubblicare niente che in futuro possa metterti in imbarazzo. Ciò che viene messo online, rimane online!

5.2.2 Il Social Network Poisoning

Con *Social Network Poisoning* si definisce uno specifico tipo di azioni malevoli messe in atto sui social: si introducono profili artefatti e relazioni inesistenti per contraffare e rendere inaffidabili le informazioni condivise.

Non essendo possibile verificare sempre e in ogni momento la veridicità dei profili degli utenti dei social, 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 e/o non congrui nel proprio profilo (*profile fuzzing*),

- l'ingresso in gruppi che non hanno a che fare con i propri interessi e relazioni, con il solo intento di fare rumore (*social graph fuzzing*).

Attenzione

Abbiamo descritto comportamenti che non è affatto difficile mettere in atto, con le finalità più disparate. Ti invitiamo a riflettere sul fatto che, anche involontarimanete, questi modi di fare possono avere conseguenze gravissime, come nei casi sempre più diffusi di cyberbullismo.

5.2.3 Strumenti per comunicazioni online sicure

In definitiva, sarebbe davvero ingenuo credere che l'utilizzo dei social network non comporti gravi rischi per la nostra sicurezza.

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.

Una nota di merito va fatta a WhatsApp che, attivando la *crittografia end to end* (E2EE) protegge la segretezza delle comunicazioni in transito, in modo che non siano visibili nemmeno da chi gestisce i server dell'azienda.

Il sistema E2EE 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 sui computer di mittente e di destinatario e non su un server esterno.

Il funzionamento della *crittografia end to end* in WhatsApp è automatico, ma se vuoi esser certo una volta per tutte dell'identità del tuo interlocutore, puoi chiedere una conferma. Dovete incontrarvi e:

1. Aprire la conversazione e toccare sulla scritta che parla della crittografia end-to-end.
2. Cliccare su *Conferma*. Viene generato un codice QR con tanti numeri, sotto, casuali, che rappresentano il codice di decriptazione.
3. Il tuo amico deve adesso scansionare il codice QR con il suo smartphone.

Facebook e la chat di Google non usano questo sistema e inoltre:

- non hanno un sistema che permetta agli utenti di identificare la vera identità delle persone con cui si sta comunicando,
- non rendono pubblico il codice di programmazione per un giudizio oggettivo da parte degli esperti.

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 E2EE, anche i dipendenti dell'azienda non potrebbero accedervi.
- Possibilità di verifica istantanea dell'interlocutore.
- Sicurezza della cronologia delle comunicazioni nel caso in cui le chiavi di crittografia venissero rubate.
- Il codice del 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.

In base a questi parametri, la EEF afferma che, come abbiamo accettato, le applicazioni di comunicazione più popolari come BlackBerry Messenger, Facebook Chat, iMessage, Skype, Snapchat, Viber e WhatsApp sono insicure.

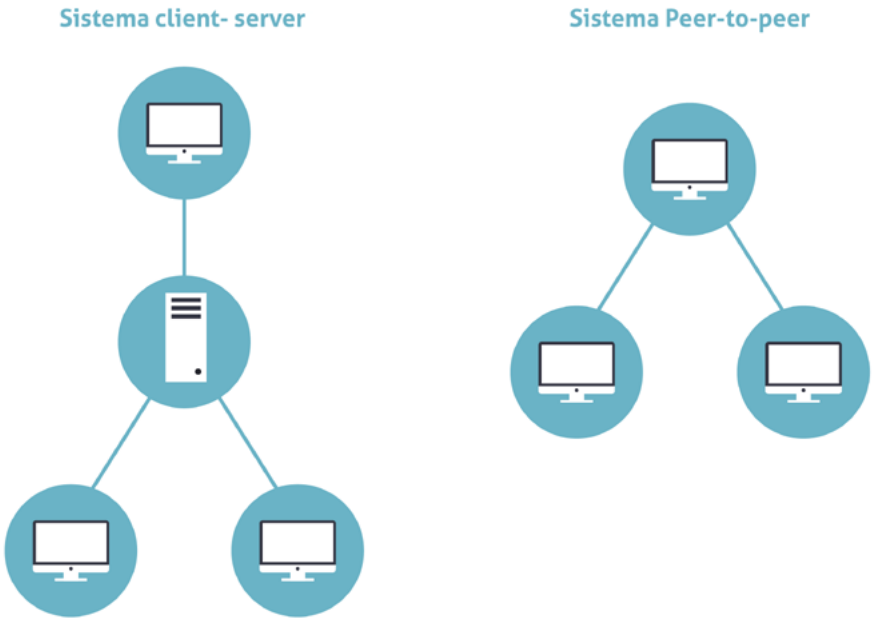
Tutte le società controllanti, fatta eccezione per Apple e WhatsApp, possono decifrare e leggere qualsiasi messaggio scambiato.
Molti sono preoccupati del fatto che governi e autorità possano richiedere le cronologie per leggere questi messaggi quando lo ritengono più opportuno. È già successo; è un tema aperto.

Preso atto di tutto ciò, puoi continuare a utilizzare i Social più diffusi (speriamo, almeno, con un po' più di accortezza) o puoi scegliere di utilizzarne altri che, invece, rispettano i parametri proposti da EEF:

1. 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.
2. Silent Circle è un'applicazione a pagamento (con abbonamento piuttosto caro) 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.
3. Signal Messenger per Android, iPhone e web è la chat cifrata che permette anche di fare telefonate protette da intercettazioni. È possibile anche inviare messaggi istantanei con testo, immagini e video nella chat.
4. Telegram non ha un punteggio perfetto ma rimane comunque un'app di messaggistica sicura quasi al 100%.
5. Wickr è un'app per Android e iPhone 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!

5.3 La tecnologia peer to peer (P2P)

Il P2P è la tecnologia tramite cui gli utenti connessi a Internet possono condividere i file archiviati sul proprio PC, come se fossero in una rete LAN.



5.7 | Sistema Client Server (a sinistra) e Sistema Peer-to-peer (a destra)

5.3.1 Che cosa è il P2P

Con il termine *peer-to-peer* (o rete paritaria o paritetica) si indica una rete in cui i nodi non sono organizzati e suddivisi in client o server, ma sono equivalenti o paritari (in inglese, *peer*).

Questo significa che ogni nodo può essere, allo stesso tempo, *cliente* e *servente* degli altri nodi (detti host) connessi, scambiando con ognuno i file archiviati.

Le applicazioni possono essere molto varie (Microsoft e Google, ad esempio, consentono a piccoli gruppi di condividere e lavorare su file online) ma questa tecnologia è utilizzata soprattutto per condividere musica, film e tanti altri contenuti, in un modo che comporta:

- rischi per la sicurezza degli utenti,
- elementi di illegalità relativi alla violazione dei diritti di *copyright* dei dati scambiati.

5.3.2 I rischi della tecnologia P2P

Vediamo con attenzione quali sono i rischi di questo sistema, per altri versi davvero democratico e universale.

Indipendentemente dall'applicazione utilizzata (eMule, Napster, MIRC ecc.), è impossibile stabilire a priori l'affidabilità del nodo da cui stiamo scaricando i dati; in pratica, non sappiamo se il PC dell'utente da cui stiamo acquisendo un film, ad esempio, sia infettato con virus o se l'utente stesso non usi questo sistema per riempirci di malware tramite cui accedere, successivamente al nostro PC.

Bisogna tener conto del fatto che, per funzionare, questi programmi richiedono spesso, ad esempio, di disattivare il *firewall*.

I file disponibili sulle reti P2P, come accennato, possono includere software piratato, materiale sprovvisto di copyright o materiale pornografico. In casi del genere, potresti incorrere in multe o in serie azioni legali.

Infine, questa attività di upload/download (denominata *File Sharing*) incrementa la mole di traffico scambiato e il carico di lavoro del nostro computer, rallentandone le prestazioni.

Da quanto detto, deriva che la cosa migliore sarebbe non utilizzare le applicazioni P2P per scambiare file.

6. SICUREZZA DEI DATI

6.1 La gestione sicura dei dati

Sappiamo che uno degli obiettivi dell'IT Security è quello di garantire l'integraità dei dati conservati sul nostro PC o nei server delle grandi aziende che fanno questo per mestiere.

In questa sezione impariamo alcune specifiche tecniche di prevenzione *fisico-materiali* dei nostri dati.

6.1.1 Le tecniche di protezione dei dati

Lo storage

Se pensi alla mole di dati creati, disponibili e scambiati ogni giorno in Internet, comprendi facilmente quanto alta sia la necessità di salvarli, in modo sicuro.

Considerate queste necessità pratiche, la tecnologia si è evoluta fino ad aggregare singole unità disco per realizzare infrastrutture in cui, in pratica, non ci sono limiti fisici alla quantità di dati caricabili.

Nello stesso tempo, per ridurre i costi di gestione, queste risorse sono state sempre più centralizzate, fino ad essere conservate su singoli dispositivi.

Con il termine *storage* (che potremmo tradurre in *sistema di archiviazione dati*) si indicano tutti i supporti hardware e software:

- Organizzati con la specifica finalità di conservare enormi quantità di informazioni in formato elettronico,
- Capaci di garantire la sicurezza delle informazioni conservate.

I diversi tipi di storage

NAS (*Network Attached Storage*). Il dispositivo è collegato a più computer messi in rete tra loro.

Questo sistema:

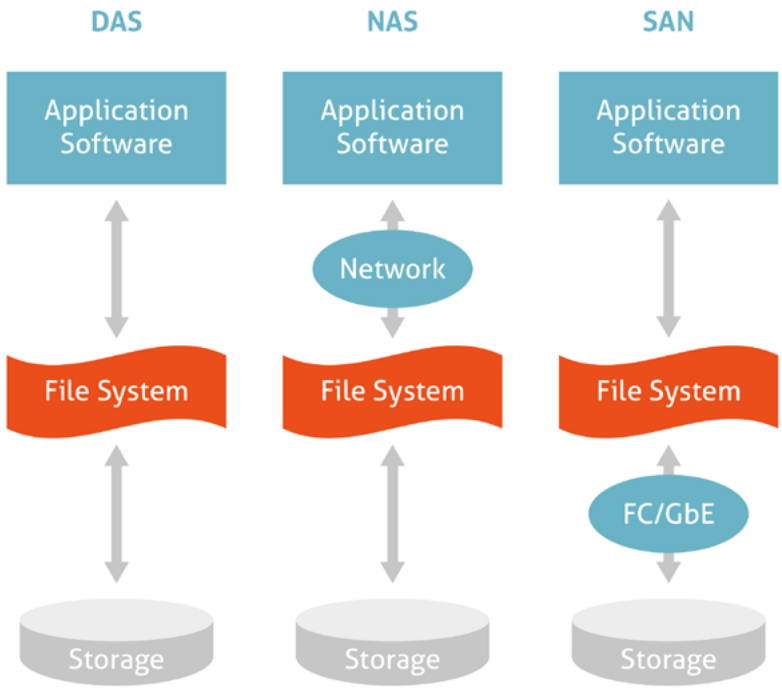
- Permette di centralizzare l'immagazzinamento dei dati in un'unità accessibile a tutti i nodi della rete e specializzata,
- Garantisce che i dati immagazzinati sia molto più al sicuro.

Lo svantaggio è che la grande quantità di dati in transito nella rete locale può determinare rallentamenti e malfunzionamenti del sistema.

DAS (*Direct Attached Storage*). Prima forma di *storage*, consiste in un dispositivo di immagazzinamento di dati che è collegato direttamente a un *server* o a un computer, non avendo alcuna connessione di Rete. Sono diverse le negatività, a confronto con i metodi più moderni: ad esempio,

- È difficile condividere i dati tra più computer.
- L'espansione dello spazio di immagazzinamento è complessa.

SAN (*Storage Area Network*). Sistema di immagazzinamento dati capace di renderli disponibili a computer connessi (normalmente a Internet), ad altissima velocità, grazie all'utilizzo della *fibra ottica* (Gigabit/sec). I vantaggi rispetto ai sistemi DAS è evidente: consente ai *server* e ai *dispositivi di storage* di avere una connettività diretta, con un'ottimizzazione dell'efficienza dello spostamento di dati e processi (come, ad esempio, il *backup* o la *replica dei dati*).



6.1 | I diversi sistemi di storage

6.1.2 Il backup dei dati

Si tratta di un aspetto davvero importante della gestione di un computer.

Siamo tutti oramai abituati a creare file, in continuazione: scattare e caricare foto, scaricare musica e video, elaborare documenti di testo, di calcolo e così via.

Sai cosa potrebbe succedere al tuo computer in caso, ad esempio, di sbalzo di tensione o di una momentanea interruzione della corrente?

A meno che tu non utilizzi un gruppo di continuità, questi eventi possono corrompere i tuoi file, anche fino a renderli irrecuperabili!

Potrebbe capitare anche che l'hard disk del tuo computer si rompa (può succedere soprattutto se lo usi tutti i giorni) o che te lo rubino (soprattutto se è un portatile).

Per evitare problemi di questo genere, è buona norma creare una copia di sicurezza dei propri dati che, in informatica, si definisce, appunto, *backup*.

È, in sostanza, una copia di riserva da cui puoi recuperare i tuoi dati in caso di perdite accidentali (che possono capitare molto più spesso di quanto si pensi).

Come è facile intuire, la copia dei dati è un'attività fondamentale soprattutto per aziende e lavoratori: i produttori di software dedicati a questa attività si impegnano per indurre gli utenti a fare più copie, senza che ciò li disturbi nell'attività quotidiana. Cercano, quindi, di:

- Ottimizzare i processi, attraverso l'individuazione più veloce degli elementi da copiare;
- Ridurre il traffico necessario a copiare i dati.

Ogni backup impegna il sistema informatico, rallentando i tempi di risposta dei computer da cui sta copiando. Per questo motivo, vari sistemi di backup vengono ancora attivati di notte, quando normalmente gli utenti non lavorano.

Come fare il backup

Una prima forma semplificata di backup è quella di copiare i file che sono sul nostro PC su un supporto esterno:

- Hard disk esterni,
- Supporti rimovibili (CD, DVD, Pen-drive USB, Schede),
- Internet, grazie al Cloud.

A prescindere dal metodo scelto, è buona norma fare almeno una copia al mese dei tuoi dati.

Il punto è che, eccezion fatta per il Cluod, con tutti gli altri supporti corriamo gli stessi rischi visti prima: danneggiamento, perdita, furto.

La soluzione a questi inconvenienti è data dal *backup Windows 10* e, cioè, dallo strumento che Microsoft ci mette a disposizione per salvare automaticamente i dati del PC, evitando di perderli nel momento in cui si dovesse verificare un guasto o altro.

Cronologia file di Windows 10

Questo strumento consente di salvare copie dei file che utilizziamo e sono conservati nelle cartelle principali di Windows: *Desktop, Documenti, Raccolte* e settaggi importanti del PC.

Per attivare la funzionalità:

1. Collegare un hard disk esterno o una penna USB.
2. Clicca su *Start* > *Impostazioni* > *Aggiornamento e Sicurezza* > *Backup*, sull'elenco che trovi sulla sinistra.
3. Clicca su *Aggiungi unità* per impostare l'hard disk esterno o la penna USB come dispositivo su cui copiare i file.

A questo punto devi selezionare i file che intendi salvare. Clicca su *Altre opzioni*: si apre l'elenco delle cartelle già inserite nella lista di backup, che potrai modificare aggiungendo o rimuovendo altre cartelle.

Sempre da questa stessa schermata, puoi impostare le tempistiche con cui verranno effettuati i backup, oltre che il tempo per cui desideri conservare i file salvati.

6.1.3 Ripristinare i file salvati

Quando vorrai recuperare i file copiati, entra nella memoria esterna: troverai le tue copie organizzate con la stessa struttura che si trova sul PC.

Puoi, quindi, ricopiare i file che ti interessano dalla memoria esterna e riportarli sul PC.

In realtà, c'è un modo più pratico:

1. Digita *Pannello di controllo* in Cortana.
2. Clicca su *Cronologia file*.
3. Clicca su *Ripristina i file personali* nell'elenco sulla sinistra, per visualizzare una finestra che contiene i tuoi documenti salvati, in ordine cronologico.

Nello stesso elenco a sinistra clicca su *Escludi cartelle* per scegliere i file che non intendi salvare (ad esempio, se hai una libreria musicale molto corposa che non vuoi tenere sull'hard disk, con questa opzione, puoi escluderla dal backup).

6.1.4 Il Backup su Mac

Su Mac si utilizza *Time Machine*, un utility tramite cui salvare dati e applicazioni su un hard disk esterno.

Clicca sull'icona dell'applicazione a forma di orologio con una freccia attorno, in alto a destra della bara dei menu e seleziona *Entra in Time Machine*.

Si apre una schermata con al centro una finestra del *Finder*. Usala per selezionare il file o la cartella da ripristinare; scegli i vari backup disponibili usando la barra temporale.

Seleziona l'elemento da ripristinare e clicca su *Ripristino*.

6.1.5 Il Cloud

Un'altra soluzione è il Cloud e, cioè, uno spazio online a tua completa disposizione, in cui trasferire e conservare file.

OneDrive, uno dei tanti servizi disponibili, è il Cloud di Windows 10.

È subito disponibile in maniera gratuita per tutti gli utenti con account Microsoft.

Se ne hai già uno per aver utilizzato lo store di Windows o Windows Phone, Hotmail, Xbox Live o Skype, quei dati di login andranno benissimo per OneDrive.

Diversamente, iscriversi alla pagina dedicata.

Creato l'account, entra nel servizio online e salva i tuoi file nella cartella di OneDrive.

Essendo online, potrai accedervi anche da altri dispositivi e PC.

Oltre alle funzioni integrate, puoi utilizzare software gratuiti molto performanti, come, ad esempio, EaseUS Todo Backup Free (compatibile anche con Windows Vista e Windows XP) o fwbackups, per chi utilizza Linux; ce ne sono, comunque, molti altri.

6.2 Il ripristino di sistema

Se continui a visualizzare messaggi di errori che fino a ieri non c'erano o hai installato una serie di programmi che credi possano aver minato la stabilità del tuo PC, puoi risolvere tutto riportando il tuo PC alle condizioni di qualche giorno fa, quando non avevi alcun problema.

6.2.1 Il ripristino su Windows 10

Hai a disposizione una funzione che ti consente di tornare indietro e ripristinare il tuo PC così come era qualche giorno, settimana o, addirittura, qualche mese fa.

1. Digita *Ripristino* in Cortana.
2. Clicca sulla voce che esce in alto, per aprire la finestra di dialogo *Ripristino* del *Pannello di Controllo*.
3. Clicca su *Apri ripristino configurazione di sistema*. Si apre una finestra. Scegli se:
   - Tornare al punto di ripristino immediatamente precedente, mantenendo selezionata l'opzione *Ripristino consigliato*.
   - Sfogliare i diversi punti di ripristino disponibili, spuntando Scegli un punto di ripristino diverso.
4. Clicca su *Avanti.*

Se hai selezionato la seconda opzione, vedrai l'elenco di tutti i punti di ripristino disponibili. Scegli *Mostra ulteriori punti di ripristino* o *Cerca programmi interessanti* per affinare la ricerca.

5. Seleziona il punto di ripristino che fa più al caso tuo, clicca su *Avanti* > *Fine* > *Si*.

L'operazione può richiedere diversi minuti.

Il PC si riavvia automaticamente e all'accesso successivo (che sarà più lento del solito) visualizzerai un messaggio che conferma il ripristino alla data che hai scelto.

Prima di iniziare, devi verificare, inoltre, che il disco su cui stai ripristinando i dati abbia dimensione uguale o superiore al disco che intendi ripristinare (questo vale anche nel secondo caso). In questa sede, ci soffermiamo sul secondo tipo di ripristino, riferendoci a quello dei soli file.

6.2.2 Il ripristino di sistema su Mac

Se vuoi ripristinare l'intero sistema del tuo Mac, devi riavviarlo in modalità ripristino.

1. Clicca sull'icona della mela in alto a sinistra, nella barra dei menu e seleziona *Riavvia*.
2. Non appena il Mac si riavvia, tieni premuto *Cmd+R* fino a quando non compare il logo di Apple.
3. Quando viene visualizzata la schermata per la selezione della lingua, clicca su *Usa l'italiano come lingua principale*.
4. Clicca sulla freccia in basso.
5. Nel menu di ripristino, seleziona *Ripristina da backup di Time Machine* e clicca su *Continua* per due volte.
6. Scegli il disco di Time Machine, clicca su *Continua* e seleziona la data del backup da ripristinare.
7. Clicca su *Continua*, seleziona il disco su cui è installato MacOS e clicca su *Ripristina* per avviare la procedura.

6.3 Eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi

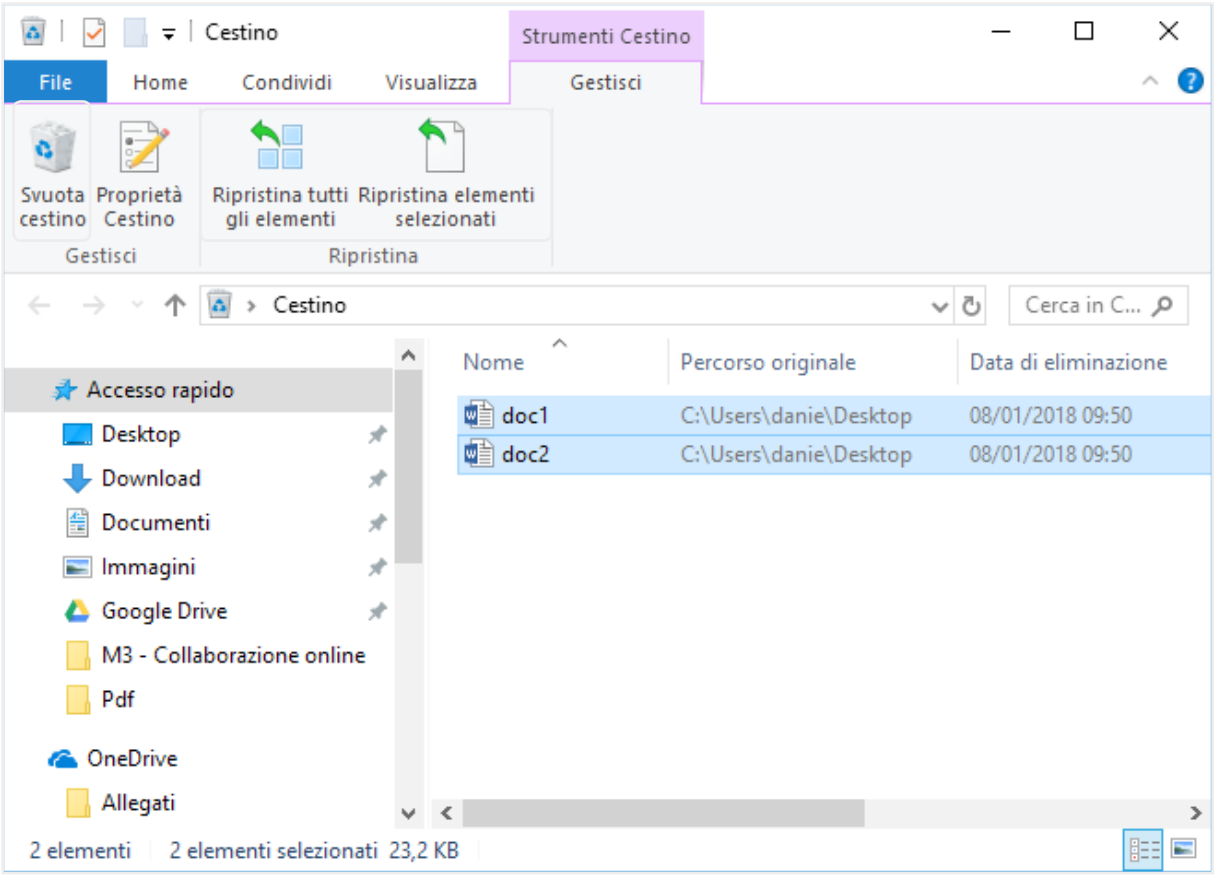
Quando un dato non ti serve più, è buona norma cancellarlo, piuttosto che intasare il tuo computer o il tuo device con file inutili che, a lungo andare, ne limitano le prestazioni.

Per farlo, spostalo nel cestino.

6.3.1 Il cestino

Il cestino è una cartella speciale che contiene tutti i file eliminati. Bada bene, però: questi file sono tutti facilmente recuperabili (tecnicamente, si dice ripristinabili).

Se vuoi ripristinare file cancellati, apri la cartella *cestino*, seleziona i file e clicca su uno dei comandi indicati di seguito.



6.2 | La cartella cestino

Per facilitare queste operazioni, ti consigliamo di visualizzare la *barra degli strumenti*, così come hai vedi nella figura precedente. Per farlo, clicca su *Gestisci* e, poi, sull'icona *freccetta in basso* sulla destra della *barra dei menu*.

Se, invece, vuoi che i file nel cestino siano rimossi definitivamente, clicca sul comando *Svuota cestino*.

Devi sapere, però, che anche dopo aver svuotato questa cartella, sul disco rimangono delle tracce che software specifici (come *Glary Utilities* e *Recuva*) possono acquisire per ricostruire integralmente o quasi i file rimossi, a seconda del tempo che passa dalla loro cancellazione e dai successivi utilizzi del computer.

6.3.2 Eliminazione definitiva dei file

Il modo più sicuro per eliminare definitivamente i file è quello che vedi raffigurato nell'immagine di fianco: forare con un trapano la memoria che li contiene! Devi, in pratica, distruggere il supporto.

Esistono, comunque, delle alternative meno cruente e invasive che assicurano una cancellazione sicura.

Glary Utilities, (lo stesso programma che può recuperare i *file*), ha uno strumento efficace per distruggerli in modo definitivo.

6.3 | Distruggere la memoria di massa

Il metodo usato (*American Dod 5220.22-M*) è sviluppato dal *Dipartimento Difesa USA* per rimuovere i dati in sicurezza.

CCleaner è un altro *software* che ti permette di cancellare (*ripulire*, come dice il nome) dal tuo computer tutti i file che non sono più utili. Ne abbiamo già fatto cenno: questo programma è in grado di cancellare anche tutti i file che registrano le tracce della tua navigazione in Internet e che vengono automaticamente salvati sul tuo PC.

Questo tipo di pulizia ha innegabili vantaggi:

- libera spazio di memoria dall'hard disk del tuo PC,
- difende la tua privacy,
- rende più veloce il sistema operativo.

SITOGRAFIA

treccani.it

motherboard.vice.com/it/read/la-storia-dei-primi-sei-anni-di-Anonymous

bpsistema.it/wifi-security-wep-wpa-e-wpa2

windows.microsoft.com/it-it/windows7/create-a-restore-point

codexsprawl.wordpress.com/tag/eavesdropping

google.it/chrome/browser/features.html#security

support.google.com/accounts/answer/6197437

support.google.com/chrome/answer/114836?visit_id=0-636491853013190018-2898132008&p=-settings_privacy&rd=1

google.it/intl/it/safetycenter/tools/#home

microsoft.com/it-it/security#Panoramica

veridium.net

spyzie.com/it/parental-controls/free-parental-control-software.html

eff.org

whatsapp.com/security

www.certipass.org

- ENTE EROGATORE DEI PROGRAMMI INTERNAZIONALI DI CERTIFICAZIONE DELLE COMPETENZE DIGITALI EIPASS
- ENTE ACCREDITATO DAL MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA PER LA FORMAZIONE DEL PERSONALE DELLA SCUOLA – DIRETTIVA 170/2016
- ENTE ISCRITTO AL WORKSHOP ICT SKILLS, ORGANIZZATO DAL CEN (EUROPEAN COMMITTEE FOR STANDARDIZATION)
- ENTE ADERENTE ALLA COALIZIONE PER LE COMPETENZE DIGITALI – AGID
- ENTE ISCRITTO AL PORTALE DEGLI ACQUISTI IN RETE DELLA PUBBLICA AMMINISTRAZIONE, MINISTERO DELL'ECONOMIA E DELLE FINANZE, CONSIP (L. 135 7 AGOSTO 2012) | MEPA
- ENTE PRESENTE SU PIATTAFORMA SOFIA E CARTA DEL DOCENTE

PER INFORMAZIONI SULLE CERTIFICAZIONI INFORMATICHE **VISITA IL SITO**

www.eipass.com