

dati di chi si collega a esse, convinto di essere stato fortunato a trovare una rete aperta con la quale collegarsi gratuitamente a Internet.

- **dirottatori di rete o "network hijacking"** (pr. *nèt-uòrc ai-giàkin*) che reindirizzano la nostra navigazione verso annunci pubblicitari e siti carichi di spyware e virus.
- **violatori di comunicazioni private o "man in the middle"** (pr. *mèn in t midòl*) che sono in grado di leggere, inserire o modificare messaggi tra due persone che stanno avendo una conversazione privata in rete attraverso un social network, una chat o altro.

### 3.2.3

**Comprendere il termine "hotspot personale"**

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

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

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

### 3.2.4

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

Vediamo, nella pratica, come **abilitare un hotspot personale con un dispositivo funzionante con il sistema operativo Android**. Le istruzioni si riferiscono alla versione 5 di Android, ma sono simili anche per versioni precedenti.

Apriamo il menu *Impostazioni*. Sotto la voce *Reti wireless* sceglieremo prima *Tethering & Reti* e poi *Hotspot Wi-Fi* facendo attenzione a toccare la scritta (evidenziata in giallo nella fig. 3.2.4a) e non il pulsante di attivazione/disattivazione del servizio (evidenziato in rosso).



FIG 3.2.4a ▶

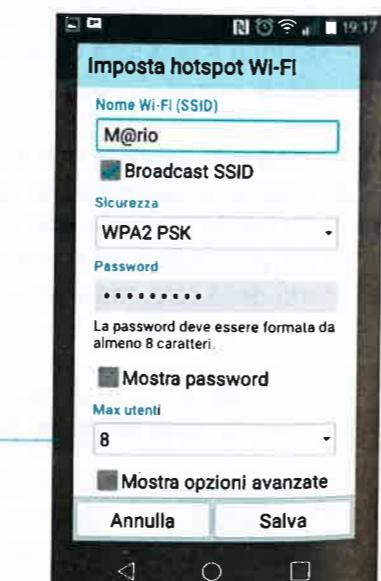


FIG 3.2.4b ▶

Nella nuova finestra che si apre dovremo cliccare su *Imposta hotspot Wi-Fi* per impostare i dati di accesso (fig. 3.2.4b):

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

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

A questo punto l'hotspot personale è stato configurato e deve essere abilitato. Torniamo perciò al menu *Tethering & Reti* e attiviamo l'*Hotspot Wi-Fi* toccando, stavolta, il pulsante di attivazione/disattivazione del servizio e non la scritta (fig. 3.2.4a).

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

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

più

**Attenzione:** prima di attivare l'hotspot personale, assicuratevi che il piano dati che avete sottoscritto con l'operatore telefonico sia predisposto per il Tethering (vale a dire la condivisione della connessione) e che non presenti costi aggiuntivi.

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

- accedere alle *Impostazioni di iOS* pigliando sull'apposito pulsante presente nella schermata principale;
- selezionare la voce *Cellulare*;
- accertarci che le opzioni *Dati cellulare* e *Abilita 4G* siano attivate;
- scorrere la schermata e piggere su *Hotspot personale* per accedere alle impostazioni della funzione di hotspot (fig. 3.2.4c);
- impostare una password rete piggiando sulla voce *Password Wi-Fi*;
- spostare su *ON* la levetta dell'opzione *Hotspot personale*.

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

Per **disattivare l'hotspot personale di iPhone** basta spostare su *OFF* la levetta dell'opzione *Hotspot personale* (fig. 3.2.4c).



▼ FIG 3.2.4c

## Sezione 4

## Controllo di accesso

## 4.1 METODI

## 4.1.1

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

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

**più**

Mentre una rete cablata (che cioè utilizza i cavi) richiede un collegamento fisico e quindi visibile tra i diversi dispositivi, le reti wireless sono raggiungibili anche da dispositivi mobili posti all'esterno dell'edificio dal quale parte il segnale radio. Rischi simili sussistono anche per le connessioni bluetooth (pr. blù-tuòt), solitamente utilizzate per collegare auricolari, cuffie o scambiare file di piccole dimensioni. Per tale motivo, il bluetooth va attivato solo per il periodo strettamente necessario, anche perché diminuisce fortemente la durata della batteria del dispositivo.

Identifichiamo i metodi più comuni ed efficaci:

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

## 4.1.2

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

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

Per ulteriore sicurezza, la one-time password è di solito trasmessa all'utente attraverso un canale differente da quello utilizzato per la trasmissione dei dati, utilizzando una autenticazione a più fattori come quella spiegata nel punto precedente. Ad esempio, se siamo collegati attraverso un computer, essa ci può essere inviata tramite SMS, posta elettronica, oppure comparire su un apposito dispositivo (fig. 4.1.2) o in una app per smartphone, forniti spesso dalle banche ai propri clienti.



▲ FIG 4.1.2

**L**o scopo di un account di rete è duplice:

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

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

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

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

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

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

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

## 4.1.3

Comprendere lo scopo di un account di rete

## 4.1.4

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

## 4.1.5

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

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

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

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

## 4.2 GESTIONE DELLE PASSWORD

### 4.2.1

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

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

più

Esistono applicazioni in grado di decodificare le password all'insaputa dei loro legittimi "proprietari". Per ridurre questo rischio **bisogna evitare che le password corrispondano**:

- a dati personali (nomi o date di nascita propri o di familiari o di persone care, numeri di telefono, targa della propria auto, ecc.);
- a sequenze prevedibili (del tipo "123456", "000000", "password", "QWERTY", "ciao", ecc.);
- a parole di uso comune, in quanto i programmi per reperire password utilizzano dizionari;
- a nomi di personaggi famosi o dei fumetti;
- a tutto o a parte del nome utente.

Infine, quando digitate la password, assicuratevi sempre di essere al sicuro da occhi indiscreti: persone esperte riescono a individuare una password anche guardando con la coda dell'occhio, senza tener conto della possibilità che si "aiutino" con piccole videocamere.

### 4.2.2

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

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

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

L'esempio più semplice è quello dei software di gestione delle password che sono integrati nei principali browser: Internet Explorer, Chrome, Edge, Firefox, ecc. Molti di noi avranno infatti notato che quando effettuiamo il login a un sito, inserendo i nostri nome utente e la password, il browser ci chiede se vogliamo che quei dati vengano memorizzati per essere poi inseriti automaticamente dal browser stesso quando ci ricollegheremo a quel sito (fig. 4.2.2).



FIG 4.2.2

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

Ad esempio, se il dispositivo fosse lasciato incustodito e acceso, oppure ci fosse rubato, estranei potrebbero accedere a siti protetti da noi visitati, utilizzandone le funzioni. Inoltre, potrebbero visualizzare l'elenco delle password memorizzate nel browser.

Inoltre, sempre più browser offrono l'utile funzione di sincronizza-

zione dei dati, che permette di ritrovare tutte le proprie impostazioni (i preferiti, la cronologia di navigazione, il database delle password inserite, ecc.) anche se accediamo al browser con altri dispositivi.

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

Vanno almeno ricordati altri due tipi di software di gestione delle password:

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

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

## Uso sicuro del Web

# Sezione 5

## 5.1

### 5.1.1

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

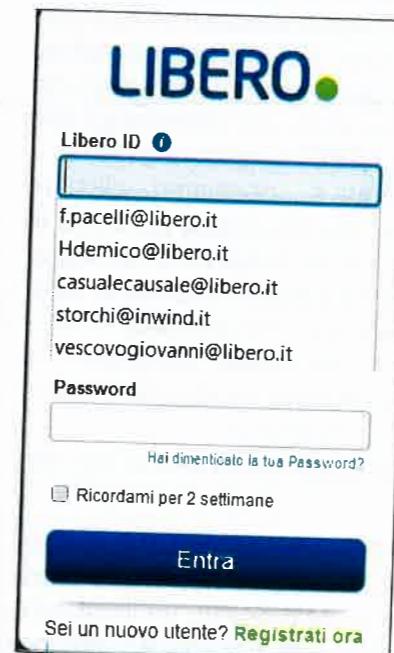
#### IMPOSTAZIONI DEL BROWSER

Quando tramite Internet dobbiamo effettuare un'iscrizione per accedere a un servizio, una richiesta per effettuare una transazione o un acquisto, occorre compilare una specie di modulo, composto da una serie di caselle nelle quali ci sono chieste delle informazioni: nome, indirizzo, ecc. Per agevolarci, il browser memorizza i dati che inseriamo, in modo da poterceli riproporre quando compilero un altro modulo.

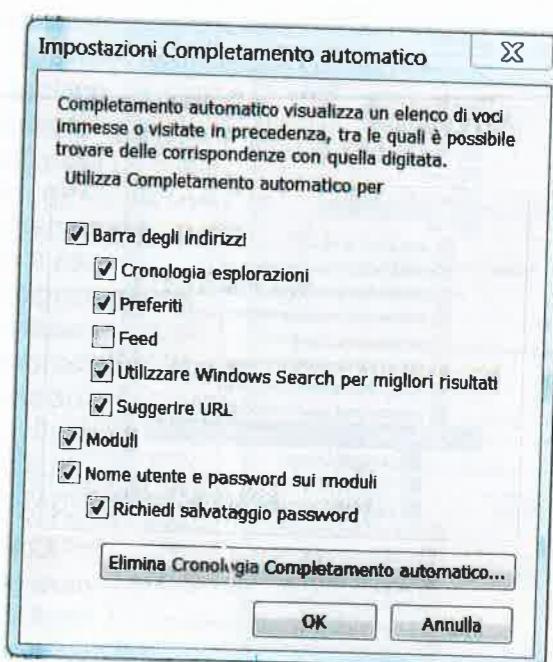
Questa funzione è indubbiamente comoda, ma può risultare pericolosa se non siamo gli unici a usare quel dispositivo. In particolar modo se utilizziamo il computer di un ufficio, di una scuola o di un qualsiasi locale dove sono disponibili computer con accesso a Internet gratuito o a pagamento, oppure se prestiamo il nostro dispositivo a un conoscente, nel momento in cui la persona estranea si accingerà a compilare un modulo, potrà prendere visione dei dati già inseriti in precedenza, che gli appariranno in un menu a discesa (fig. 5.1.1a).

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

In *Internet Explorer* occorre cliccare prima sull'icona *Strumenti* (in alto a destra, ha la forma di un ingranaggio), poi su *Opzioni Internet*, quindi sulla scheda *Contenuto*, al cui interno troveremo la sezione *Completamento automatico* col rispettivo pulsante *Impostazioni* che ci consente di aprire la finestra *Impostazioni Completamento automatico* (fig. 5.1.1b) al cui interno potremo scegliere se abilitare o disabilitare il completamento dei moduli ed anche, specificatamente, il nome utente e la password nei moduli.



▲ FIG 5.1.1a



▲ FIG 5.1.1b

In **Microsoft Edge** occorre selezionare *Altro* (il pulsante che si trova all'estrema destra della barra degli indirizzi e che rappresenta tre puntini sospensivi), poi *Impostazioni*, quindi *Visualizza impostazioni avanzate*, dove potremo attivare o disattivare l'opzione *Salva i dati immessi nei moduli*.

Se utilizziamo **Google Chrome** dovremo cliccare prima sul pulsante *Menu* (in alto a destra), poi su *Impostazioni* per aprire l'omonima pagina nella quale, dopo aver cliccato su *Mostra impostazioni avanzate*, troveremo la sezione *Password e moduli* dove poter attivare o disattivare il completamento automatico dei moduli e il salvataggio delle password.

Con **Firefox** dovremo cliccare prima su *Apri menu* (pulsante in alto a destra) e poi su *Opzioni*. Nell'omonima finestra che si apre, cliccheremo su *Privacy* e attiveremo, alla voce *Impostazioni cronologia, Utilizza impostazioni personalizzate*. A quel punto potremo scegliere se utilizzare sempre la navigazione anonima (che non conserva traccia dei siti visitati) oppure quali parti della navigazione (cronologia dei siti visitati, dati dei moduli, cronologia delle ricerche) vogliamo memorizzare e quali no. Per disattivare il salvataggio delle password dovremo scegliere, nella finestra delle *Opzioni*, la scheda *Sicurezza*, nella quale potremo disattivare la funzione *Ricorda le password dei siti* oltre a poter visualizzare le password memorizzate per decidere quali cancellare e quali conservare, cliccando sul pulsante *Password salvate*.

## 5.1.2

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



FIG 5.1.2a ➤



Con **Microsoft Edge** occorre selezionare prima il pulsante *Hub* (nella barra degli indirizzi, rappresenta tre linee ed è evidenziato in giallo nella fig. 5.1.2b), poi *Cronologia* (il pulsante che rappresenta

un orologio, evidenziato in rosso), infine *Cancella tutta la cronologia* (evidenziato in verde nella fig.). È possibile anche aprire direttamente la cronologia premendo contemporaneamente i tasti *Ctrl* e *H*.

Con **Chrome** si clicca prima su *Menu* (ultimo tasto in alto a destra) e poi su *Cronologia* ed è sempre valida la scorciatoia attraverso i tasti *Ctrl* e *H* premuti contemporaneamente.

Con **Firefox** la procedura è *Apri menu > Cronologia* e anche in questo caso è possibile aprire la finestra premendo contemporaneamente *Ctrl* e *H*.

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

Se si desiderano cancellare queste informazioni con **Internet Explorer** (ad es. per evitare che altre persone possano visualizzarle, in particolar modo se abbiamo navigato utilizzando un dispositivo non nostro, ma di un amico, di un collega, di un laboratorio di informatica o di un Internet Point) occorre cliccare prima su *Strumenti* (l'icona a forma di ingranaggio) e poi su *Opzioni Internet*. Nella parte centrale della finestra che compare (fig. 5.1.2c) cliccate sul tasto *Elimina* che si trova nella sezione *Cronologia esplorazioni*. Accanto al pulsante *Elimina* troviamo altre opzioni: la casella *Elimina la cronologia al momento di uscire*, che cancella l'elenco dei siti visitati ogni volta che chiudiamo il browser e il pulsante *Impostazioni* che ci permette, tra l'altro, di scegliere per quanti giorni saranno conservate le pagine web nella *Cronologia*.

più

Se, invece, vogliamo cancellare dalla *Cronologia* solo un sito web visitato possiamo portarci sulla voce che ci interessa in *Cronologia*, cliccare con il pulsante destro del mouse e scegliere dal menu che compare la voce *Elimina*. Con la stessa modalità possiamo cancellare il contenuto delle voci presenti nella cronologia di un determinato periodo, ad esempio: *Oggi*, *Ultima settimana*, *2 settimane fa*, ecc.

Con **Microsoft Edge**, selezioneremo prima il pulsante *Altro*, poi *Impostazioni* e quindi (nella se-



FIG 5.1.2b

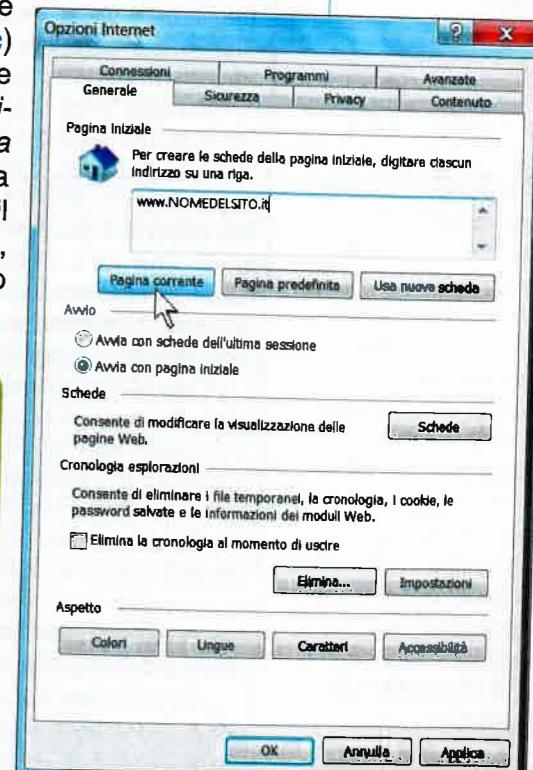


FIG 5.1.2c

zione *Cancella dati delle esplorazioni*) Scegli gli elementi da cancellare per selezionare o deselectionare cosa vogliamo cancellare tra: *Cronologia esplorazioni; Cookie e dati di siti web salvati; Dati e file memorizzati nella cache; Cronologia download; Dati moduli; Password*.

Se utilizziamo **Chrome** la procedura è *Menu > Cronologia >* cliccare sul pulsante *Cancella dati di navigazione* e scegliere quali elementi cancellare.

Con **Firefox** bisogna scegliere la voce *Cancella cronologia recente* che compare nel menu *Cronologia*, al quale si accede dal pulsante *Apri menu*. Anche in questo caso potremo scegliere tra diverse opzioni per cancellare tutti i dati o solo alcuni a nostra scelta. È anche possibile accedere a *Cancella cronologia recente* premendo contemporaneamente i tasti *Ctrl Maiusc e Canc.*

più

**Il cookie** (pr. *cuki*, sign. "biscottino") è un file di piccole dimensioni, contenente dei dati, che viene creato da alcuni siti ai quali ci collegiamo e registrato nella memoria del dispositivo che stiamo utilizzando.

Quando si torna a visitare quel sito, il cookie trasmette al sito una serie di informazioni di tipo statistico e commerciale riguardante l'utente. Un esempio classico è quello delle "pubblicità mirate", che fanno comparire in molti siti che visitiamo pubblicità di prodotti riguardanti ricerche che abbiamo effettuato o siti che abbiamo visitato.

I cookie, inoltre, possono servire a memorizzare alcuni dati (per non doverli reinserire ogni volta che ci si ricollega a un sito) o le preferenze dell'utente riguardo la configurazione dei servizi offerti dal sito. Alcuni siti richiedono che il meccanismo dei cookie sia attivo. Se, ad esempio, effettuiamo operazioni bancarie tramite Internet, il server della banca, per rispettare le regole di sicurezza, è costretto ad interrogare continuamente il computer chiamante. A questo punto è il cookie che la banca ha depositato in quel dispositivo a fornire a ogni richiesta le generalità del dispositivo stesso. Se nel browser tutti i cookie sono stati bloccati, il dialogo tra il nostro dispositivo e il server della banca non può stabilirsi.

Il cookie in sé non è pericoloso, ma memorizza le nostre navigazioni, per cui occorre sapere come **consentire o bloccare i cookie**.

Con **Explorer**, dovremo cliccare prima su *Strumenti* (l'icona a forma di ingranaggio), poi su *Opzioni Internet* e quindi sulla scheda *Privacy*. In questa scheda è possibile scegliere, muovendo il cursore scorrevole, tra i vari livelli, che sono (dal basso verso l'alto): *Accetta tutti i cookie, Bassa, Media* (è il livello predefinito), *Media alta, Alta, Blocca tutti i cookie*. Nella stessa finestra, cliccando sul pulsante *Siti* è possibile indicare degli indirizzi web specifici per i quali consentire o bloccare i cookie.

Con **Microsoft Edge** dovremo selezionare prima il pulsante *Altro* (ultimo nella barra degli indirizzi), poi *Impostazioni* e quindi *Visualizza impostazioni avanzate*. Scorrendo il riquadro laterale che compare, troveremo la sezione *Cookie* con tre possibili scelte: > *Blocca tutti i cookie; Blocca solo i cookie di terze parti; Non bloccare i cookie*.

Se utilizziamo **Chrome**, dopo aver cliccato sul pulsante *Menu* (in alto a destra) sceglieremo *Impostazioni > Mostra impostazioni avanzate* (in basso) > *Impostazioni contenuti* (nella sezione *Privacy*) per accedere all'omonima finestra nella quale abiliteremo con un clic la voce *Blocca cookie di terze parti e dati dei siti*.

Con **Firefox** la procedura è: *Apri menu > Opzioni > scheda Privacy >* alla voce *Impostazioni cronologia* scegliere *utilizza impostazioni personalizzate > disattivare Accetta i cookie dai siti*.

## NAVIGAZIONE SICURA IN RETE

5.2

5.2.1

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

▼ FIG 5.2.1



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

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

Esistono anche reti aperte che permettono la connessione libera, ma occorre tener presente che in questo caso altri utenti potrebbero essere in grado di rilevare tutte le operazioni che eseguiamo: siti visitati, documenti aperti, nomi utente e password utilizzati.

Per sapere se una rete è sicura o meno, possiamo portare il puntatore su una delle reti disponibili: comparirà un riquadro con le principali caratteristiche, tra cui la presenza e il tipo dell'eventuale protezione (fig. 5.2.1).

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

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

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

Se cerchiamo notizie prima di effettuare un viaggio all'estero è ben

5.2.2

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

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

**più**

Viviamo in un flusso continuo di informazioni, per cui è fondamentale sapere quali sono quelle più accurate, credibili e importanti per noi. Solo in questo modo possiamo difenderci da un carico di informazioni inutili o fuorvianti che ci arrivano ogni giorno attraverso strumenti tecnologici di ogni tipo.

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

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

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

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

Altro elemento fondamentale è la presenza o meno dell'**indicazione delle fonti dalle quali sono tratte le informazioni riportate**, perché questo consente di individuare l'origine dell'informazione e di verificarne validità e attendibilità. Ovviamente, le fonti indicate devono essere conosciute o almeno verificabili. Se, ad esempio, in un sito web trovo un'informazione del tipo "nel 2012, le vendite delle auto in Italia sono diminuite del 19,87% rispetto all'anno precedente" l'attendibilità è ben diversa se è indicata come fonte una pagina web che mi porta al "Rapporto ACI-Censis 2012" o piuttosto se non è indicata nessuna fonte o un riferimento del tutto generico del tipo "come ha affermato il telegiornale".

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

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

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

La maggior parte delle pagine web adotta il cosiddetto "protocollo http" (pr. *acca-ti-ti-pi*), nel quale i dati sono trasmessi senza alcuna cifratura.

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

**più**

Lo stesso browser ci indica se ci troviamo in questi che sono definiti **siti web sicuri**, facendo comparire nella barra degli indirizzi l'**immagine di un lucchetto chiuso** (fig. 5.2.2a: il puntatore indica proprio l'icona del lucchetto). Inoltre, nella barra degli indirizzi il nome del sito sicuro non comincia con **http** ma con **https** (pr. *acca-ti-ti-pi-esse*): la "s" finale è l'iniziale di *secure*, vale a dire "sicuro" (fig. 5.2.2a). Questo indica che i dati scambiati in quella pagina sono criptati.



FIG 5.2.2a

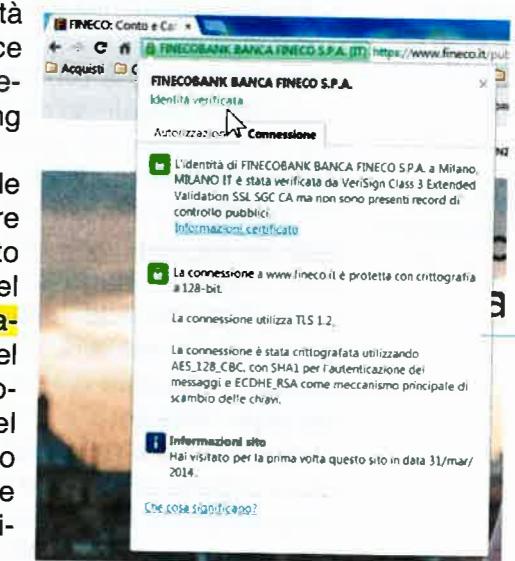


FIG 5.2.2b

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

Per visualizzare il certificato di sicurezza, le generalità del sito e l'ente certificatore occorre cliccare due volte sull'icona del lucchetto chiuso che compare nella barra di stato del browser. Questa procedura è detta **validazione** perché, quando clicchiamo sull'icona del lucchetto, viene inviato al sito un testo crittografato con la chiave pubblica riportata nel certificato. A quel punto, solo se il sito è quello originale, potrà rispondere con la sua chiave privata per far comparire il messaggio di verifica dell'identità (fig. 5.2.2b).

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

Ad esempio, è possibile ricevere mail apparentemente inviate da banche, siti di vendita on-line o altre aziende famose che ci invitano a collegarci al loro sito per risolvere problemi di sicurezza (ad es. c'è bisogno di confermare o cambiare la propria password) o per approfittare

**più** La scritta "http://" è quella che precede il "www" e in genere non compare neppure più nei browser (pr. *bräuser*), che sono le applicazioni che utilizziamo per navigare in Internet.

### 5.2.3

Comprendere il termine "pharming"

di eccezionali offerte (ad es. solo per quel giorno, chi ricaricherà la propria carta di pagamento di una piccola somma di denaro, riceverà in omaggio una somma pari o addirittura maggiore), oppure per effettuare operazioni importanti e non rimandabili (fig. 5.2.3).

Oggetto: Postepay- telegramma urgente . - 69562-2863-77284  
 Da: alerta12715@13252-secure.BPOLit +  
 A: <f.pacelli@libero.it> +  
 Gentile Cliente Poste Italiane ,  
 Notifica invio telegramma (n. di accettazione: 82150-86376-41495)  
[Accedi telegramma urgente online](#)

▲ FIG 5.2.3

Queste mail contengono al loro interno uno o più link che apparentemente dovrebbero condurci al sito di quella banca o di quella azienda. In realtà, il link ci condurrà a un falso sito che cerca di imitare il più possibile quello originale, per spingerci a inserire con fiducia i nostri dati personali, che ovviamente saranno immediatamente intercettati da questi pirati informatici, che potranno adoperarli a loro piacimento.

Altre volte, il link scarica nel nostro dispositivo elettronico un malware che consente al pirata informatico di accedere al nostro dispositivo. I provider filtrano la maggior parte di questo tipo di mail, i programmi antivirus bloccano buona parte dei malware, gli stessi browser ci segnalano se il sito al quale stiamo per collegarci non risulta affidabile ma resta comunque alta la possibilità di capitare in questi falsi siti (ad es. cliccando su un link contenuto in un altro sito).

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

#### 5.2.4

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

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

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

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

*Internet Explorer* include già un controllo dei contenuti. Per attivarlo occorre cliccare, nell'ordine, sull'icona *Strumenti*, poi su *Opzioni Internet* e, nella scheda *Contenuto*, sul pulsante *Family Safety* (pr. *fàmili sèifì*; sign. "controllo genitori"). Anche altri browser offrono soluzioni simili: *Chrome* consente di creare "utenti supervisionati" le cui attività possono essere controllate dal supervisore, che può anche decidere di limitare alcuni domini; *Firefox* rileva se sono attivati il *Controllo genitori* in *Windows* o i *Controlli censura* nei sistemi *Apple* più recenti e, se li trova in funzione, filtra automaticamente i contenuti per adulti per ogni sito che si visita.

## Comunicazioni

### Sezione 6

#### 6.1

##### 6.1.1

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

#### POSTA ELETTRONICA

La posta elettronica è un mezzo di comunicazione importante per molti privati e spesso indispensabile per molte imprese. Esistono, però, numerosi rischi legati all'uso della posta elettronica.

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

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

più

Esistono diversi sistemi di cifratura dei messaggi di posta elettronica. Tra i più sicuri vi è quello a **doppia chiave asimmetrica**, nel quale ogni utente ha una coppia di chiavi di crittografia, una privata e una pubblica. Dalla chiave privata può essere generata una sola chiave pubblica. Il messaggio reso illeggibile dal mittente con la chiave privata, potrà essere letto dal destinatario utilizzando la chiave pubblica corrispondente. In questo modo, il destinatario avrà la sicurezza dell'identità del mittente.

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

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

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

più

Anche legalmente la validità della firma digitale è pari a quella di una firma autografa su carta, in quanto risponde a tre principi:

1. autenticità: il destinatario può verificare l'identità del mittente;
2. non ripudio: il mittente non può disconoscere il documento che ha firmato;
3. integrità: il destinatario non può modificare il documento firmato dal mittente.

#### 6.1.2

Comprendere il termine "firma digitale"

**6.1.3**

**Identificare i possibili messaggi fraudolenti o indesiderati**

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

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

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

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

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

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

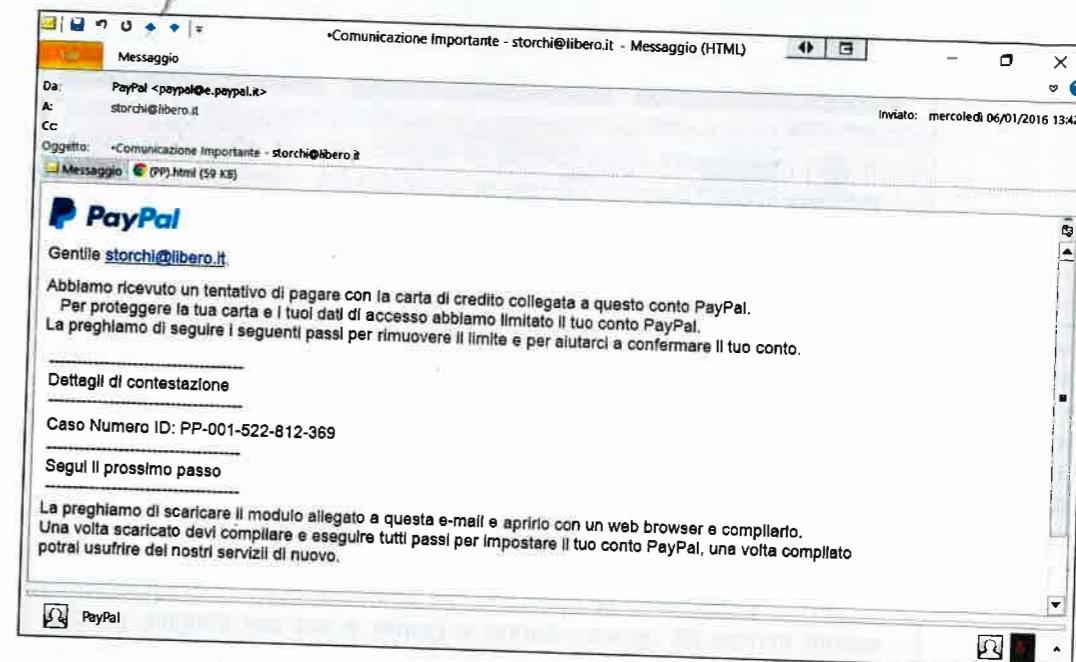
**6.1.4**

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

**C**on il termine **phishing** (pr. fīscing, sign. "gettare l'amo") si indicano le tecniche usate da alcuni truffatori per ottenere l'**accesso illegittimo a informazioni personali e riservate, mediante l'utilizzo di messaggi di posta elettronica falsi** ma modificati in modo da sembrare inviati da aziende note. Tramite questi messaggi, l'utente è ingannato e portato a rivelare dati personali come numero di carta di credito, password o altri dati personali.

Ad esempio, si riceve una mail apparentemente proveniente dal servizio clienti di una banca, di un sito di commercio elettronico, da *PayPal*, *Poste Italiane*, ecc. (dei quali in genere compaiono anche i loghi e i marchi originali) nella quale si avvisa di un problema di verifica dati, di un con-

trollo a campione, del rischio di disattivazione del nostro conto, della vittima di un premio o di una somma di denaro, con la richiesta di collegarsi immediatamente al sito della società, cliccando su un link contenuto nella mail, per poi inserire alcuni dati personali come account o numero di carta di credito. Cliccando sul link, la persona visualizza sul proprio schertranello. Una volta comunicati i propri dati personali o finanziari, questi vengono usati dai truffatori che hanno spedito il messaggio per effettuare acquisti o trasferire somme di denaro a spese del malcapitato.



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

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

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

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

**6.1.5**

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

**più** La Polizia di Stato ha creato un "Commissariato online" raggiungibile all'indirizzo [www.commissariatodips.it](http://www.commissariatodips.it) dove è possibile denunciare i reati informatici, avviando una procedura che in ogni caso richiede poi di recarsi presso un Ufficio di Polizia per completare e convalidare la denuncia.

The screenshot shows the homepage of the Commissariato di P.S. website. At the top, there's a banner with the text "LIVELLO DI ALLERTA ALTO per l'ESPANSIONE ATTENZIONE! VENDITA ABUSIVA DI TITOLI DI MAGGIO FERROVIARI DI TRENTALIA". Below the banner, there are three main sections: "Informati" (Information), "Domanda" (Question), and "Collabora" (Collaborate). Each section has a brief description and a call-to-action button. The "Informati" section says "Leggi le notizie per essere sempre informato sui nostri servizi" and has a "PUBBLICATO IL NUOVO QUIZ" section. The "Domanda" section says "Hai un dubbio? Compa il formiga sotto e chiedi ai nostri esperti" and has a "Richiedi informazioni" button. The "Collabora" section says "Se ti trovi in presenza di un reato informatico, entra in contatto con noi" and has buttons for "Segnala online", "Denuncia per reati telematici", and "Denuncia per furto o smarrimento".

### 6.1.6

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

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

**più** Costituiscono un pericolo anche link a pagine web, che possono portare all'esecuzione di malware. Un esempio, sono mail apparentemente inviate da giovani donne e giunte a noi per sbaglio, perché indirizzate a loro amici, nelle quali spesso si invita a cliccare su un link per vedere contenuti erotici. In realtà, cliccando sul link, nel proprio computer verrà caricato un malware.

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

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

**più** Anche se l'antivirus è aggiornato e segnala che l'allegato è pulito, occorre sapere che tra l'uscita di un nuovo malware e la disponibilità dell'aggiornamento che lo riconosce, passa qualche ora. Durante questo periodo, l'antivirus può dunque segnalarti che un file è pulito anche quando, in realtà, è infetto. Per questo motivo, se un eventuale blocco del computer causerebbe serie ripercussioni al vostro lavoro o al vostro studio, è consigliabile aprire immediatamente gli allegati solo se si tratta di file che si aspettava di ricevere. Anche se il file è stato inviato da una persona conosciuta e fidata, si può chiedergli conferma del fatto che voleva inviarvelo, prima di aprirlo. Negli altri casi, meglio attendere il giorno dopo per verificare che l'antivirus aggiornato confermi l'assenza di malware.

## RETI SOCIALI

### 6.2

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

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

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

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

Per il fatto stesso di mettere in comunicazione milioni di persone, Internet amplifica dei rischi presenti anche nella vita reale, per cui è bene navigare utilizzando sempre una buona dose di prudenza.

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

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

Anche la pubblicazione di immagini personali sui siti di reti sociali richiede una certa cautela: se esse ritraggono anche altre persone,

### 6.2.1

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

legalmente esse dovrebbero essere informate del fatto e dare la loro approvazione. Anche in altri casi, le immagini pubblicate possono rappresentare un pericolo; negli USA, ad esempio, alcuni ladri utilizzano le foto pubblicate nelle reti sociali per identificare e studiare le abitazioni che possono rappresentare un buon obiettivo per i loro furti.

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



È fondamentale tener presente che tutto quello che inseriamo nel Web può restarci per sempre: testi, foto e quant'altro, perché anche se eliminiamo un nostro intervento del quale ci pensiamo, copia dello stesso rimane a disposizione dell'autorità giudiziaria nei server della società che gestisce la comunità online, senza considerare che chiunque può aver effettuato una copia del nostro intervento prima della sua cancellazione. Dobbiamo, perciò, essere sempre consapevoli che, anche a distanza di molto tempo, quei testi o quelle immagini potrebbero essere letti o viste proprio da chi non vorremo.

## 6.2.2

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

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

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

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

## 6.2.3

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

FIG 6.2.3a



Vediamo come procedere per applicare le **impostazioni degli account di reti sociali**. In **Facebook**, occorre accedere alla sezione **Privacy** (generalmente indicata dal simbolo di un lucchetto chiuso, collocato in alto a destra, come nella fig. 6.2.3a, evidenziato dal cerchio giallo) e poi scegliere la voce **Vedi altre impostazioni** (evidenziata in rosso nella fig. 6.2.3a) per aprire la pagina **Impostazioni sulla privacy** e

strumenti (fig. 6.2.3b) e chi potrà vedere i messaggi che postiamo, chi può contattarci, chi può cercarci, ecc.

È anche possibile **modificare le impostazioni di privacy per singoli post** utilizzando due icone presenti nella finestra dei nuovi post (evidenziate nella fig. 6.2.3c):

permette di attivare/disattivare l'indicazione della posizione nel post che stiamo per pubblicare;

permette di scegliere chi potrà vedere il contenuto del post (e degli eventuali allegati) che stiamo per pubblicare: tutti, solo gli amici, solo gli amici più stretti, ecc.



FIG 6.2.3c

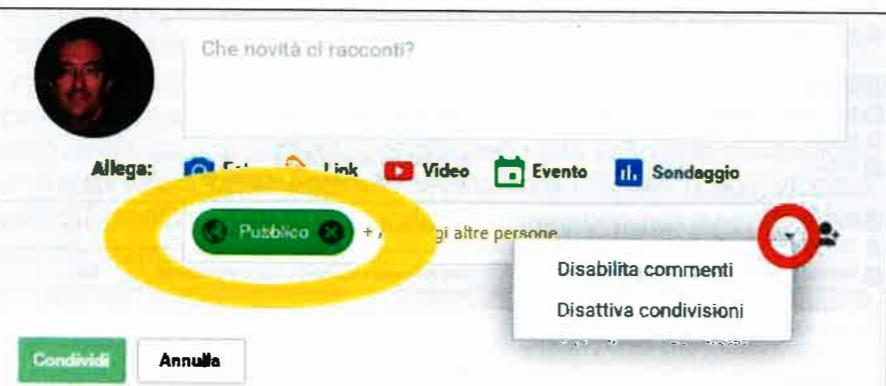
La procedura è abbastanza simile anche per altre reti sociali. Ad esempio, se utilizziamo **Google+** dovremo selezionare **Impostazioni** (l'icona a forma di ingranaggio, generalmente presente a sinistra, evidenziata nella fig. 6.2.3d)) per poi scegliere le opzioni relative alla riservatezza del proprio account (chi potrà vedere i contenuti che pubblichiamo, chi potrà commentarli) e alla localizzazione geografica.

Anche con **Google+** possiamo modificare le impostazioni anche di un singolo post:

- cliccando sul pulsante verde con il mappamondo

FIG 6.2.3d

(evidenziato in giallo nella fig. 6.2.3e) potremo scegliere chi potrà vedere il messaggio che stiamo pubblicando e gli eventuali allegati; ■ cliccando sulla freccetta rivolta verso il basso (evidenziata in rosso nella fig. 6.2.3e) potremo vietarne i commenti o le condivisioni.



#### 6.2.4

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

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

Per il fatto stesso di mettere in comunicazione milioni di persone, Internet amplifica dei rischi presenti anche nella vita reale, per cui è bene navigare utilizzando sempre una buona dose di prudenza, facendo

più

Le notizie false diffuse tramite Internet (principalmente con l'utilizzo della posta elettronica e delle reti sociali) sono chiamate **bufale** (in inglese *hoaxes*, pr. *óxis*, sign. "scherzi" o "imbrogli"). Esse si propagano attraverso il passa-parola, cercando di spingere chi le legge a dividerle con altre persone di sua conoscenza.

Un esempio sono gli appelli a favore di persone in fin di vita (bambini malati terminali, persone per le quali si cerca una cura per una malattia rara oppure un donatore), di condannati a morte, oppure i messaggi che invitano a non aprire certe mail in quanto conterebbero pericolosissimi virus informatici (generalmente inesistenti), invitando a trasmettere l'avviso a tutti quelli che conosciamo.

Possiamo quindi parlare di una specie di versione tecnologia delle vecchie "catene di Sant'Antonio": lettere che venivano spedite tramite la posta tradizionale, nella quale il destinatario era invitato a ricopiare la stessa lettera in un certo numero di copie per poi spedirla a suoi conoscenti; in questo modo si sarebbero avverati i suoi desideri, in caso contrario sarebbero accadute terribili disgrazie.

In altri casi la "bufala" può nascondere delle truffe, in particolare quando contiene promesse di facili guadagni o richieste di denaro.

Una buona norma, quando si legge o si riceve un appello, è quello di controllarne la veridicità sui siti Internet che raccolgono le "bufale" che circolano in Rete, ad es.: [www.trendmicro.com/vinfo/hoaxes/hox.asp](http://www.trendmicro.com/vinfo/hoaxes/hox.asp) e [www.attivissimo.net/antibufala/index.htm](http://www.attivissimo.net/antibufala/index.htm)

attenzione a non rendere pubbliche informazioni personali che riguardano noi o persone a noi vicine, perché questo potrebbe essere sfruttato da malintenzionati per forme di molestia, prepotenza o ricatto. Teniamo sempre ben presente che le persone nella realtà possono essere molto diverse da come si descrivono in rete: spesso non abbiamo modo di sapere se la persona che si presenta a noi come un ragazzo o una ragazza sia davvero tale o, piuttosto, un adulto con cattive intenzioni.

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

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

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

#### VOIP E MESSAGGISTICA ISTANTANEA

#### 6.2.5

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

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

Utilizzando una applicazione specifica (ad es. *WhatsApp*, pr. *uòts app*) o un analogo servizio integrato in un'applicazione (ad es. la chat di *Facebook* o la messaggistica istantanea di *Skype*, pr. *skàip*), sullo schermo del nostro dispositivo compare un riquadro ("contact list", pr.

#### 6.3

#### 6.3.1

Comprendere le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP), quali malware, accesso da backdoor

*contact list*) nel quale è possibile sapere quante e quali persone che conosciamo e il cui nome abbiamo memorizzato nell'applicazione, sono in quel momento collegate come noi in rete.

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

L'instant messaging è utilizzato principalmente dagli adolescenti, ma ne è diffuso l'uso anche tra gli adulti, alcuni dei quali utilizzano questo servizio anche al lavoro per comunicare e scambiare file con colleghi e clienti.

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

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

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

### 6.3.2

Riconoscere i metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP

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

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

## 6.4 DISPOSITIVI MOBILI

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

Attualmente, i dispositivi mobili maggiormente diffusi sono smartphone e tablet, entrambi dotati di collegamento a Internet e di uno schermo sensibile al tocco del dito e perciò detto "touchscreen" (pr. *täuc-scrin*, con la "c" pronunciata come nella parola "cena"), sul quale compare una tastiera virtuale quando è necessario digitare caratteri o parole.

**L**e applicazioni per dispositivi mobili vanno scaricate da siti definiti **app store** (pr. *app stör*). Ogni sistema operativo possiede uno o più **app store ufficiali**; i più utilizzati sono:

- *Play Store* e *Android Market* per il s.o. *Android*;
- *Apple App Store* per il s.o. *iOS*;
- *Windows Store* per i s.o. *Windows* dedicati ai dispositivi mobili;
- *App World* (pr. *app uòrlid*) per i dispositivi *Blackberry* (pr. *blèk-bèrr*).

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

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

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

### 6.4.1

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

### 6.4.2

Comprendere il termine "autorizzazioni dell'applicazione"



FIG 6.4.2

Dopo aver scaricato un'applicazione per dispositivo mobile e subito

prima di avviare il processo di installazione, il sistema operativo ci

mostra una schermata nella quale sono elencate le diverse autorizzazioni richieste dall'applicazione (fig. 6.4.2).

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

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

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

### 6.4.3

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

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

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

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

Occorre prestare particolare attenzione alle seguenti autorizzazioni:

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

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

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



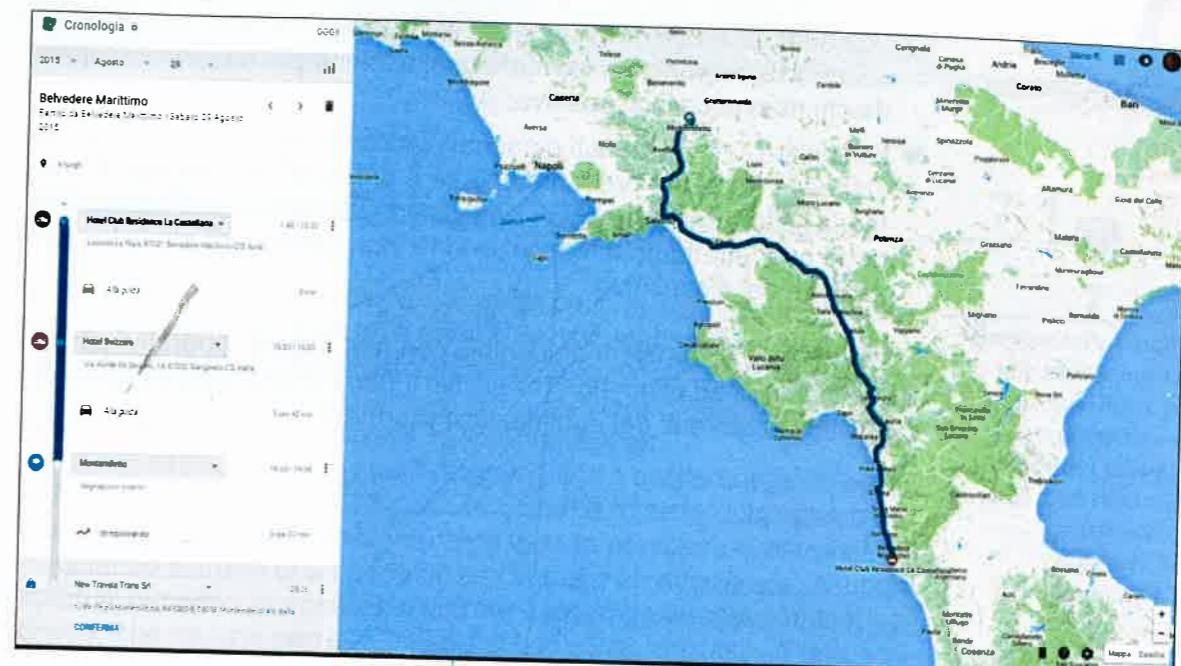
Un paio di esempi pratici serviranno a farci comprendere quanti dati personali conserviamo nei nostri dispositivi mobili, a volte ignorandolo.

Se utilizziamo un dispositivo *Android* (ma anche se utilizziamo *Google Maps* con altri dispositivi) e se abbiamo accettato al primo avvio del dispositivo di abilitare la segnalazione della posizione, possiamo collegarci a questo indirizzo web: [www.google.com/maps/timeline](http://www.google.com/maps/timeline) e rivedere su una cartina tutti i posti in cui siamo stati da quando abbiamo attivato quel dispositivo, giorno per giorno e ora per ora, anche per diversi mesi o anni (fig. 6.4.3).

Da notare che anche se non abbiamo abilitato il GPS, il dispositivo riesce a localizzarci (anche se con minore precisione) utilizzando il segnale telefonico.

Un'altra applicazione molto diffusa, *WhatsApp*, richiede tra le autorizzazioni necessarie al suo funzionamento, quella di accedere – anche più volte il giorno – all'elenco dei nostri contatti, per individuare nuovi numeri e inviare e ricevere messaggi con loro.

Inoltre, per leggere i messaggi di stato pubblicati su *WhatsApp*, basta inserire nella rubrica il numero di telefonino della persona che ci interessa. Infine, le foto e i video che riceviamo durante le nostre conversazioni, sono scaricate in automatico sul nostro dispositivo, con problemi di privacy e di esaurimento della memoria del dispositivo.



▲ FIG 6.4.3

### 6.4.4

**Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile.**

Praticamente tutti i sistemi operativi per dispositivi mobili (*Android*, *iOS*, *Windows 10*, ecc.) consentono di effettuare alcune operazioni sul dispositivo anche se l'abbiamo smarrito o se ci è stato rubato. Sono però necessarie alcune condizioni, in genere (ma non sempre) attivate automaticamente:

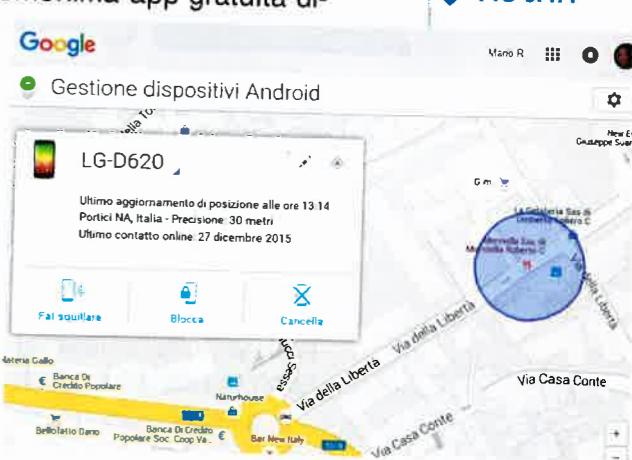
- il dispositivo deve essere associato a un nostro account;
- sul dispositivo deve essere attivata la funzione necessaria alla sua localizzazione;
- il dispositivo deve essere dotato di connessione a Internet.

Se perdiamo un dispositivo *Android*, ad esempio, dovremo accedere con un altro dispositivo al nostro account *Google* e utilizzare la funzione Gestione dispositivi *Android* o scaricando l'omonima app gratuita disponibile sul *Play Store*, oppure collegandoci all'indirizzo [www.google.com/android/devicemanager](http://www.google.com/android/devicemanager) (fig. 6.4.4).

A questo punto potremo:

- localizzare il dispositivo su una mappa;
- farlo squillare ininterrottamente per circa cinque minuti, cliccando due volte sul pulsante *Fai squillare*;
- bloccarlo, procedendo a una disattivazione remota, scegliendo il pulsante *Blocca* e impostando una password che sarà poi necessaria per lo sblocco.

▼ FIG 6.4.4



Volendo, è anche possibile far comparire un messaggio sullo schermo e comunicare un numero di telefono per essere contattato da chi ritrovasse il dispositivo;

- cancellare tutti i contenuti personali, cliccando due volte sul pulsante *Cancella*. Teniamo presente che se è presente una scheda di memoria, alcuni dati potrebbero non essere cancellati e soprattutto che, dopo aver effettuato la cancellazione, non funzionerà più la localizzazione del dispositivo.

Simili sono le funzioni disponibili con altri sistemi operativi per dispositivi mobili, ad esempio *Trova il mio iPhone* offerta gratuitamente da *Apple* agli acquirenti dei suoi dispositivi portatili.

## Gestione sicura dei dati

## Sezione 7

### MESSA IN SICUREZZA E SALVATAGGIO DI DATI

#### 7.1

#### 7

#### 7.1.1

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

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

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

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

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

più

In particolare, nel caso di dispositivi che prevedono l'inserimento di una scheda telefonica (cellulari, smartphone, alcuni tablet, ecc.), occorre ricordare che esiste un codice identificativo unico per ogni telefonino. Tale codice si chiama IMEI, è costituito da 15 cifre ed è riportato sulla confezione del dispositivo, ma può essere anche ricavato dal dispositivo stesso: digitando \*#06# (come se si stesse componendo un numero telefonico) apparirà sul display il codice IMEI, da ricopiare e conservare. In caso di perdita del cellulare, smartphone o tablet, comunicando questo codice al proprio gestore telefonico, è possibile impedire l'utilizzo del telefono da parte di altre persone. Allo stesso modo vanno tempestivamente segnalati al proprio gestore telefonico lo smarrimento o il furto della tessera (la SIM card) contenuta nel dispositivo, per bloccare il traffico telefonico e recuperare il credito rimanente.



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

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

### 7.1.2

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

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

Per questi motivi è fondamentale abituarsi a effettuare periodicamente **copie di sicurezza o backup** (pr. *bekäp*) di file la cui perdita potrebbe causare danni o difficoltà (documenti, immagini, ecc.) su sistemi di memoria di massa, in modo da poter recuperare i dati in caso di perdita o danneggiamento degli stessi sul proprio dispositivo. Come **supporti di memoria** si utilizzano principalmente penne USB, dischi fissi esterni, CD, DVD. Nelle grandi aziende si continuano talora a usare le data cartridge (pr. *déita cáratreig*, con la "g" finale pronunciata come nella parola "gelato"), che consistono in cartucce a nastro magnetico, dotate di elevate capacità di memorizzazione.

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

### 7.1.3

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

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

In questo modo, si può procedere a un backup completo a intervalli medio-lunghi, mentre con maggiore frequenza si effettuano dei backup incrementali.

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

Inoltre, i supporti di memoria sui quali sono realizzate le copie di sicurezza dei dati devono essere rimovibili, in modo da essere

più

Si distingue il "backup completo" (che effettua una copia di tutti i dati contenuti nel computer) dal "backup in aggiornamento" o "backup incrementale" (nel quale vengono aggiornati solo i dati modificati o creati dall'utente nel periodo trascorso dall'ultimo backup). In questo modo, si può procedere a un backup completo a intervalli medio-lunghi, mentre con maggiore frequenza si effettuano dei backup incrementali.

conservati in luoghi sicuri e diversi da quelli dove solitamente si trova il dispositivo. In questo modo, in caso di furto o danneggiamento del dispositivo dovuto a eventi di forza maggiore (ad esempio per un incendio o un allagamento che colpisce il locale dove si trova il computer) le copie di backup non faranno la stessa fine.

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

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

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

Gli stessi sistemi operativi (ad esempio Windows, Android, Apple OS e iOS, Linux) integrano già questo tipo di applicazioni:

- in Windows, questo programma è raggiungibile da *Pannello di controllo > Sistema e sicurezza > Backup e ripristino*;
- in Android si trova generalmente in *Impostazioni > Backup e ripristino*;
- nei sistemi Apple, è possibile utilizzare sia iCloud sia iTunes per memorizzare dati e applicazioni contenute nel dispositivo;
- in Linux Ubuntu, si può digitare "backup" nella Dash (pr. *dàsc*, con la "sc" pronunciata come nella parola "scena"), che si apre cliccando sul pulsante di Ubuntu nella barra di sinistra.

Ecco, ad esempio, la procedura necessaria per effettuare il primo backup di una unità disco, utilizzando come sistema operativo Windows 10 oppure Windows 7:

1. apriamo il *Pannello di controllo* digitando il suo nome nella casella di ricerca e scegliendo il primo risultato; con Windows 7 possiamo cliccare pulsante *Start* e poi su *Pannello di controllo*;
2. nella sezione *Sistema e sicurezza* clicchiamo sulla voce *Esegui backup del computer*;
3. nella finestra *Backup o ripristino dei file* che compare, clicchiamo sul pulsante *Configura backup* per aprire l'omonimo riquadro;
4. scegliamo in quale unità disco intendiamo salvare il nostro backup (disco fisso esterno, chiave USB, scheda di memoria, CD, DVD, ecc.) e clicchiamo sul pulsante *Avanti*;

### 7.1.4

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

5. inseriamo un segno di spunta in *Selezione automatica* per effettuare la copia di sicurezza dei dati presenti in cataloghi, desktop e cartelle predefinite di Windows (se preferiamo scegliere manualmente le cartelle da salvare, scegliendo *Selezione manuale* potremo indicare gli elementi di cui vogliamo eseguire il backup);
6. cliccando sul pulsante *Avanti* potremo verificare le impostazioni del backup: se esse soddisfano le nostre esigenze, cliccando su *Salva impostazioni ed esegui backup* avvieremo la procedura.

**Importante:** la volta successiva, se non vorremo modificare le impostazioni del backup, basterà cliccare direttamente sul pulsante *Esegui backup* che troveremo nella finestra *Backup o ripristino dei file*, al posto della voce *Configura backup*.

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

### 7.1.5

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

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

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

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

Ecco, ad esempio, la procedura necessaria per effettuare il ripristino di una unità disco, utilizzando come sistema operativo Windows 10 oppure Windows 7:

1. apriamo il *Pannello di controllo* digitando il suo nome nella casella di ricerca e scegliendo il primo risultato; con Windows 7 possiamo cliccare pulsante *Start* e poi su *Pannello di controllo*;
2. nella sezione *Sistema e sicurezza* clicchiamo sulla voce *Esegui backup del computer*;
3. nella finestra *Backup o ripristino dei file* che compare, clicchiamo sul pulsante *Ripristina file personali* che troviamo in basso a destra;

4. sarà visualizzata la finestra *Ripristina file* (v. fig. 7.1.5a), nella quale dovremo selezionare quali file intendiamo ripristinare, utilizzando i pulsanti che compaiono a lato:
  - *Cerca* per individuare i file attraverso un motore di ricerca;
  - *Cerca file* per selezionare i file attraverso una ricerca tra le cartelle;
  - *Cerca cartelle* per individuare e selezionare intere cartelle da ripristinare;
5. una volta selezionati i file o le cartelle da ripristinare (cliccando rispettivamente sul pulsante *Aggiungi file* oppure *Aggiungi cartella*), clicchiamo sul pulsante *Avanti*;
6. sceglieremo in quale cartella intendiamo ripristinare i file ed avviamo la procedura cliccando sul pulsante *Ripristina*.

**Importante:** la procedura di ripristino può richiedere parecchio tempo, durante il quale il computer deve rimanere acceso e collegato alla memoria esterna nella quale è presente il file di backup da ripristinare.

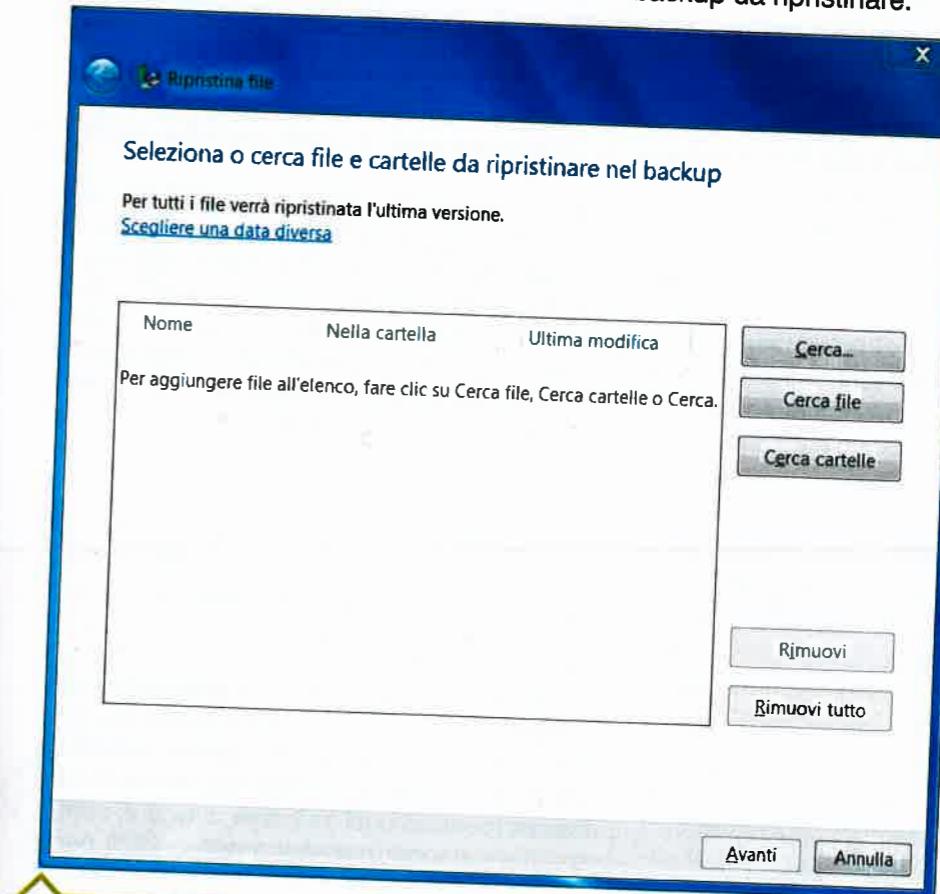


FIG 7.1.5a

**più** È consigliabile provare, almeno una volta, ad effettuare le operazioni di validazione e ripristino dei dati anche se non si è verificato il danneggiamento o la perdita degli stessi. In questo modo potremo apprendere la procedura e verificare il suo corretto funzionamento, anche perché può capitare un errore di scrittura o di procedura per cui un backup sembra essere stato creato regolarmente ma in realtà è inservibile.

## 7.2 CANCELLAZIONE E DISTRUZIONE SICURA

### 7.2.1

Distinguere tra cancellare i dati ed eliminarli in modo permanente

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

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

*più*

Infatti, quando cancelliamo un file, un gruppo di file o una cartella, il sistema operativo in realtà non cancella nulla, ma etichetta semplicemente come utilizzabile lo spazio fisico occupato nella memoria dai file che si è chiesto di cancellare. Sin quando questo spazio non verrà interamente sovrascritto da nuovi dati, quelli precedenti potranno essere recuperati, parzialmente o totalmente.

Anche se formattiamo un supporto di memoria come hard disk, chiave USB o scheda di memoria scegliendo l'opzione "formattazione rapida", i dati presenti non vengono in genere cancellati, ma solo etichettati come cancellabili.

Principalmente negli Stati Uniti, alcuni malintenzionati vanno alla ricerca di vecchi computer appartenuti ad aziende o uffici (a volte fingendo di raccoglierli per scopi umanitari) in modo da poter recuperare in essi i dati solo cancellati ma non distrutti. Utilizzano poi le informazioni raccolte in tal modo o per frodi telematiche, o per furti di identità, oppure per veri e propri ricatti nei confronti dei precedenti proprietari dei dispositivi, invitati a pagare per evitare che informazioni che possono danneggiare le aziende o la dignità di singole persone siano rese pubbliche attraverso Internet.

### 7.2.2

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

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

Noi, infatti, spesso dimentichiamo la quantità di dati personali che sono memorizzati

*più*

Anche se non fa parte del programma di esame per il conseguimento dell'ECDL, ricordiamo di fare molta attenzione quando prestiamo un dispositivo o una memoria di massa (pensiamo all'abitudine diffusa di dare ad altre persone una nostra penna USB per scambiare dei file), in quanto una persona malintenzionata può facilmente e velocemente effettuare copia dei nostri dati personali, oppure involontariamente danneggiarli o distruggerli. Persone più esperte, inoltre, possono approfittare della disponibilità temporanea di un dispositivo o di una memoria di massa per caricare in essi dei malware in grado di raccogliere e trasmettere nostri dati privati.

in un dispositivo o in una memoria di massa: da foto a conversazioni telematiche, dalla cronologia dei siti che abbiamo visitato a copie di documenti di identità, dai numeri delle ultime conversazioni telefoniche ai messaggi di testo inviati e ricevuti, ecc.

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

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

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

**P**er cancellare definitivamente i dati è necessario utilizzare metodi specifici. Esaminiamo quelli più diffusi e facilmente utilizzabili.

**Triturazione dei documenti cartacei** attraverso l'utilizzo di "trita documenti" o "distruggi documenti" (esistono anche modelli molto economici) che riducono in striscioline o coriandoli i fogli.

**Distruzione delle memorie di massa o dei dispositivi** che si è sicuri di non voler più utilizzare, vendere o regalare, utilizzando un martello o un trapano che danneggino in modo irreparabile le memorie. Nel caso di CD, DVD e schede di memoria è sufficiente piegarle più volte sin quando non si spezzano. Ovviamente si tratta di operazioni da praticare con attenzione, per evitare di farsi male.

**Smagnetizzazione** (o "degausser", pr. *degausser*) attraverso apparecchi che generano campi magnetici in grado di rendere inutilizzabili le memorie di massa. Questa è una pratica solitamente utilizzata da grandi aziende e non da privati.

**Cancellazione definitiva dei dati** grazie a programmi che dopo aver cancellato i file, sovrascrivono più volte lo spazio di memoria da loro precedentemente occupato, in modo da rendere impossibile ogni recupero.

*più*

A titolo di esempio, riportiamo alcuni dei programmi (gratuiti o scaricabili in versioni demo funzionanti) più utilizzati nei diversi sistemi operativi:

- Windows: Eraser; RightDelete; Freeraser.
- Android: CleanMaster; History Eraser.
- OS: TrashMe.
- iOS: iErase e SafeEraser.
- Linux Ubuntu: Shred; Wipe; Bleachbit.

### 7.2.3

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

### 7.2.4

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