Uso sicuro del web

Navigare in siti sicuri

La rete internet, inizialmente, era concepita come strumento di ricerca di informazioni. L'utente esercitava un ruolo passivo. Non interagiva con le pagine web ma si limitava al reperimento e alla consultazione dei dati di suo interesse. Da parecchi anni, con l'avvento del Web 2, l'utente di internet è diventato attivo: pubblica materiale proprio, inserisce informazioni, effettua acquisti, ecc. Addirittura gestisce il proprio conto bancario.
È evidente che tutto questo richiede che le pagine web dove si effettuano queste operazioni devono garantire un livello di sicurezza elevato per prevenire il furto di informazioni così rilevanti.

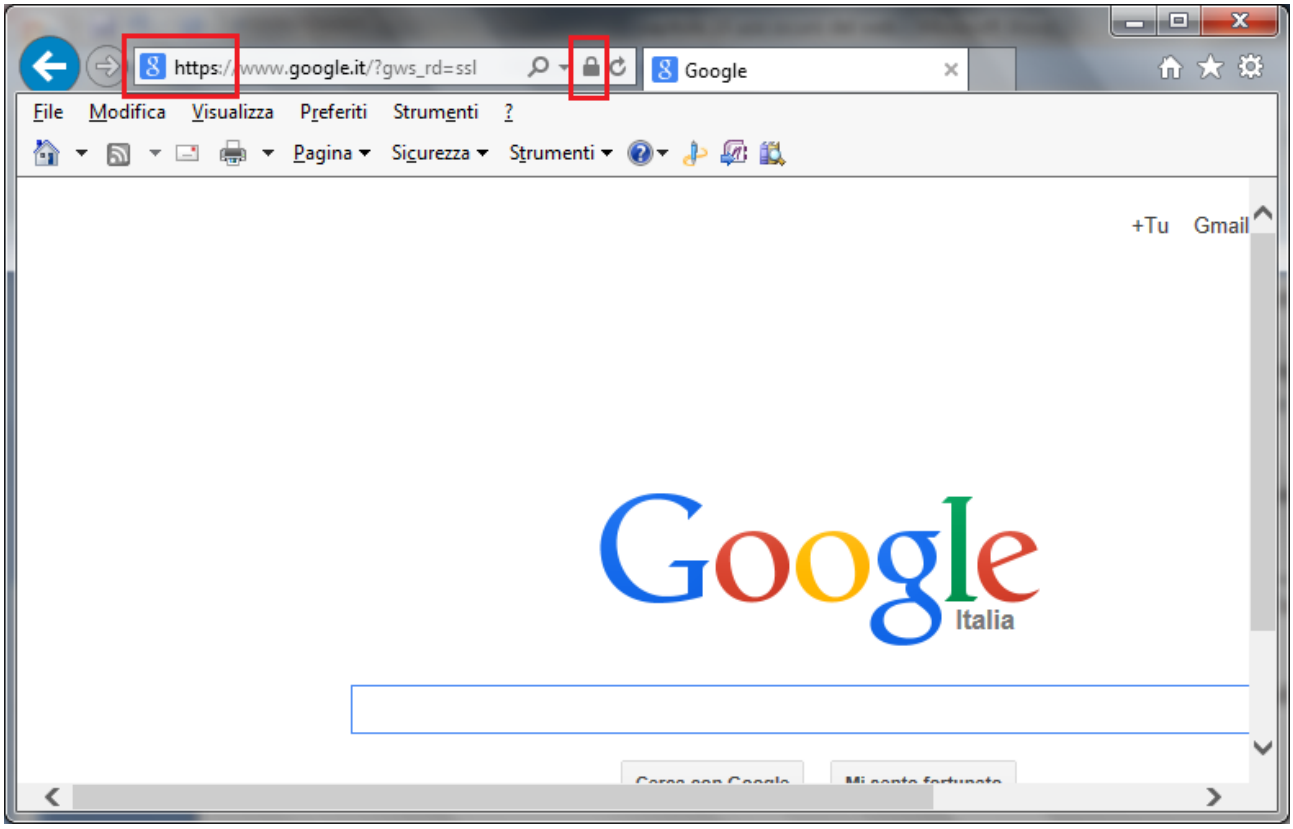
Identificazione di un sito web sicuro. I certificati digitali

Ci sono dei siti internet impostati in modo da impedire l'accesso da parte di utenti non autorizzati: ad esempio siti di home banking, acquisti on line, registrazione esami universitari, ecc.
Questi siti Web sono denominati **protetti**. La protezione avviene con l'utilizzo dei **certificati**.
Un certificato è un documento digitale che consente di verificare l'identità di una persona o un sito web. I certificati vengono rilasciati da società denominate **Autorità di certificazione**. Queste autorità stabiliscono e verificano l'autenticità delle chiavi pubbliche appartenenti a persone o altre autorità di certificazione e verificano l'identità di una persona o organizzazione che richiede un certificato.
Ci sono due tipi di certificati:

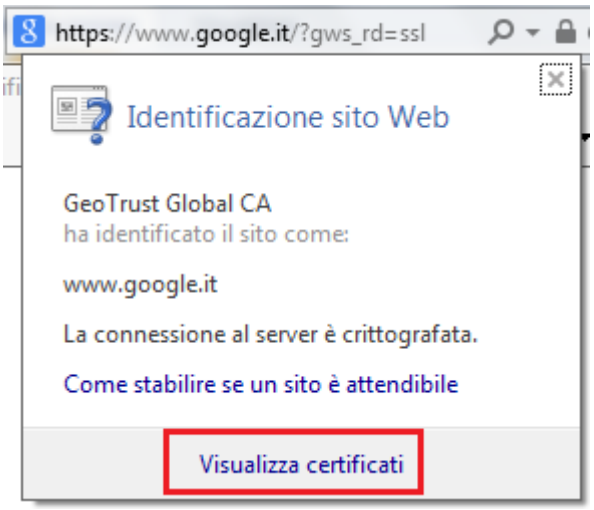
1. Un certificato personale consente di verificare l'identità dell'utente e viene utilizzato quando si inviano informazioni personali tramite internet a un sito web che richiede un certificato per verificare l'identità dell'utente. È possibile provare la propria identità con una chiave digitale privata di tipo hardware o software.
2. Un certificato di un sito web consente di identificare l'autenticità di un sito web specifico e di verificare che l'identità del sito protetto originale non venga assunta da un altro sito web. Quando si inviano informazioni personali in internet, è opportuno controllare il certificato del sito web per assicurarsi di comunicare con il sito previsto.

I certificati sono generalmente forniti agli utenti in automatico quando si utilizza un sito web sicuro per transazioni commerciali o bancarie online o si desidera crittografare un file. Se si desidera un certificato per uso personale, ad esempio per proteggere la posta elettronica mediante una firma digitale, si può contattare un'autorità di certificazione e richiedere un certificato.
Riassumendo, i certificati sono principalmente utilizzati per verificare l'identità di una persona o per autenticare un servizio.

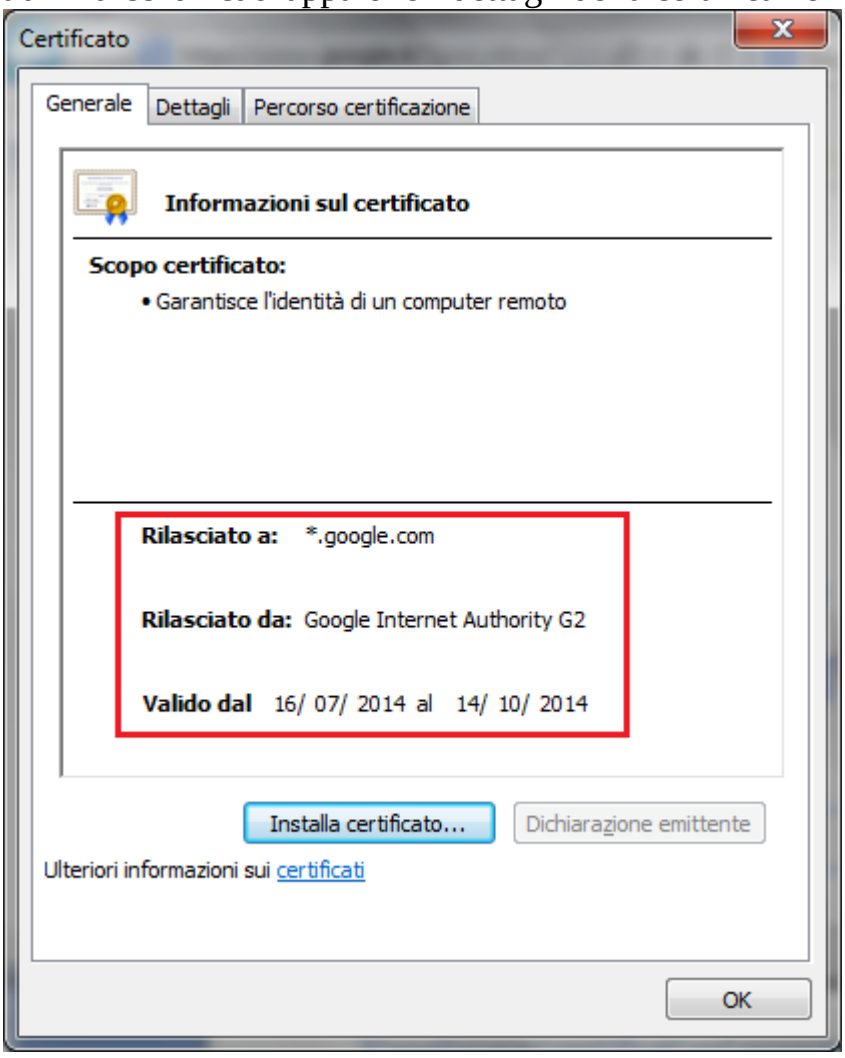
Quando si visita un sito Web protetto, il sito invia automaticamente il proprio certificato all'utente, crittografando (cioè scrivendo le informazioni in modo cifrato) le informazioni.
In Internet Explorer, nel caso di sito protetto, è visualizzata un'icona a forma di lucchetto nella barra degli indirizzi. In figura la pagina web di Google.



L'indirizzo della pagina inizia con la sigla **https** (Hyper Text Transfer Protocol Secure), invece che il "classico" http. Significa che il sito trasmette i dati dopo averli cifrati con una chiave robusta in modo che il solo sito web che li riceve e li trasmette sia in grado di decodificarli. La "s" significa "sicuro".
Facendo clic sul lucchetto, appare il rapporto sulla sicurezza relativo al sito Web con le informazioni contenute nel certificato.



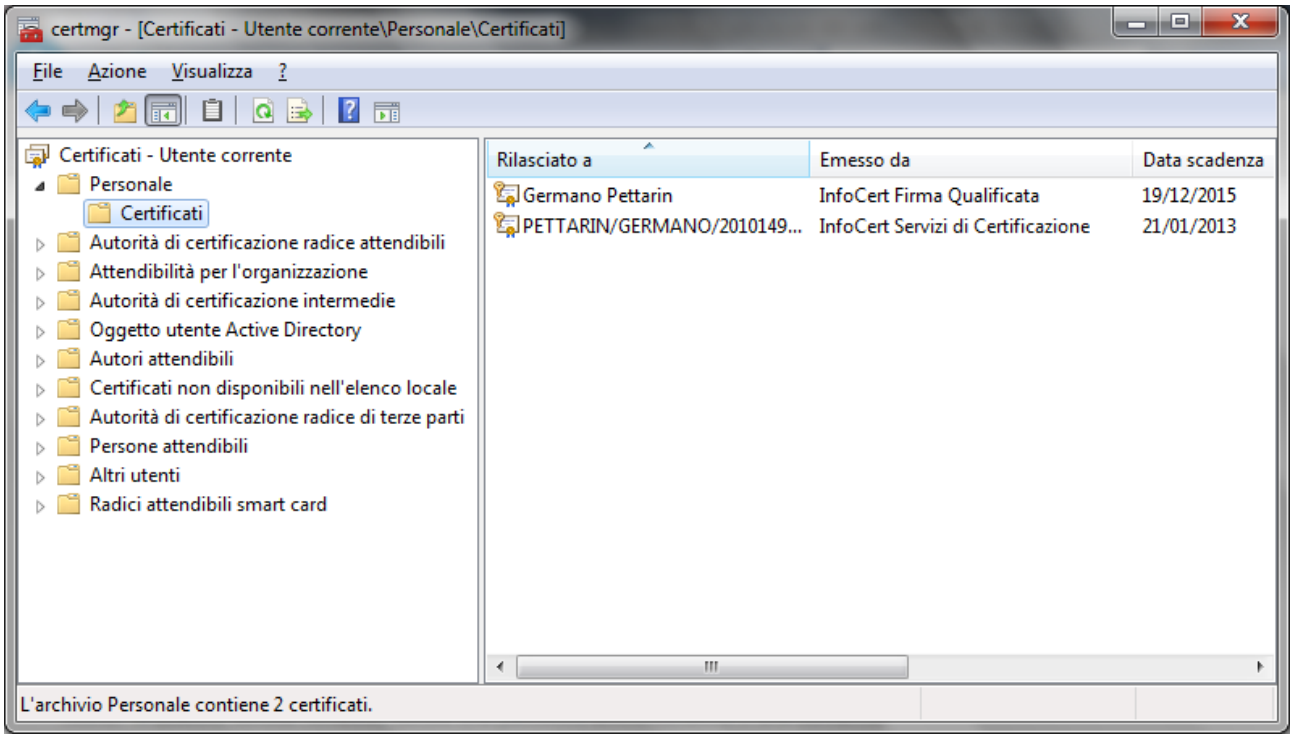
Con un clic su **Visualizza certificati** appaiono i dettagli della certificazione.



Sono specificate le informazioni di identificazione dell'autorità di certificazione e la data di inizio e la data di fine della validità, che rappresentano i limiti del periodo di validità. Un certificato è valido esclusivamente per il periodo specificato. Trascorso il periodo di validità, il soggetto del certificato scaduto dovrà richiederne uno nuovo.

Visualizzare i certificati nel proprio computer

È possibile visualizzare i certificati presenti nel computer con il **Gestore certificati**: è necessario essere connessi al computer come amministratore.
Per aprire Gestore certificati, fare clic sul pulsante **Start**, digitare **certmgr.msc** nella casella di ricerca e premere INVIO. Può essere richiesta una password amministratore o una conferma.



Il Pharming

Il **pharming** è una tecnica per impadronirsi dei dati personali di un utente, principalmente i dati bancari, simile al **phishing**.

Nel caso del pishing si hanno delle e-mail (o SMS) con falsa intestazione della banca, contenenti un link di collegamento a un "sito clone" (apparentemente identico al sito originale) e la richiesta di accedervi con le motivazioni più disparate: un movimento bancario non autorizzato, la verifica dell'estratto conto, un bonifico da confermare, ecc. Se si clicca sulla richiesta, appare una falsa pagina di accesso al conto corrente online, del tutto simile a quella vera. I dati saranno registrati dai truffatori per poi accedere al conto e ed effettuare operazioni illecite. Per raggiungere il maggior numero possibile di utenti, la stessa falsa e-mail (o SMS) è inviata a moltissimi indirizzi diversi, di clienti e non clienti, in maniera simultanea e pressoché casuale.

Nel pharming quando si digita l'indirizzo web della propria banca, o si clicca sul relativo link, si viene indirizzati in automatico al sito "clone" anche in questo caso, nel momento in cui si inseriscono i dati bancari personali, i truffatori li copiano per utilizzarli in un secondo tempo per operare sul conto corrente.

Questa tecnica opera associando all'indirizzo alfanumerico del sito un indirizzo IP diverso, quello del sito "clone". L'utente non ha strumenti per rendersi conto della differenza se non controllare il certificato digitale della pagina che utilizza il protocollo https.

One-time password

Come si intuisce dalla traduzione in italiano, una **One-Time Password** (password usata una sola volta, OTP) è una password che è valida solo una volta, per una singola sessione di accesso o una singola operazione. Gli algoritmi di generazione delle OTP in genere fanno uso di numeri casuali.

Utilizzando una OTP si possono evitare i problemi di violazione di una tradizionale password statica. Abbiamo visto come quest'ultima possa essere forzata con attacchi a forza

bruta, con software che generano tutte le possibili combinazioni di numeri e lettere. Nel caso delle OTP, dato che il valore è continuamente modificato, se un malintenzionato riesce ad conoscere una OTP già utilizzata per accedere a un servizio o eseguire una transazione, non può utilizzarla, in quanto non è più valida.
Chiaramente una OTP non può essere creata e memorizzata da una persona. Di solito, si usa un dispositivo elettronico di dimensioni ridotte (token OTP) con un display che visualizza la password generata di volta in volta.

Normalmente la OTP è una password aggiuntiva al nome utente e password utilizzati per accedere a un servizio.

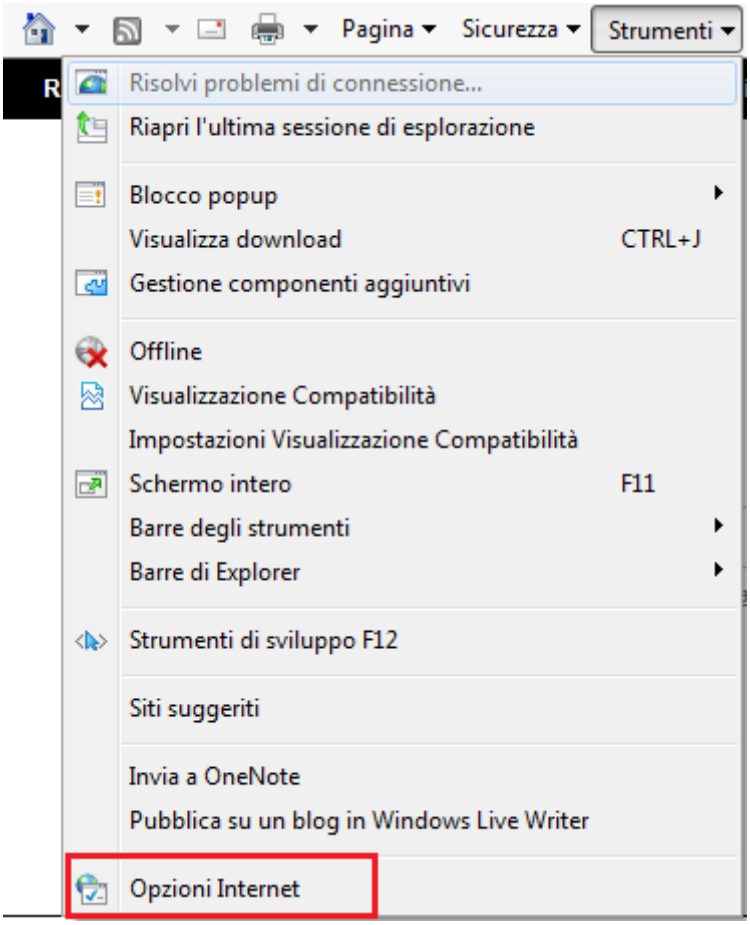
Impostare il browser per navigare in sicurezza

Opzioni di protezione

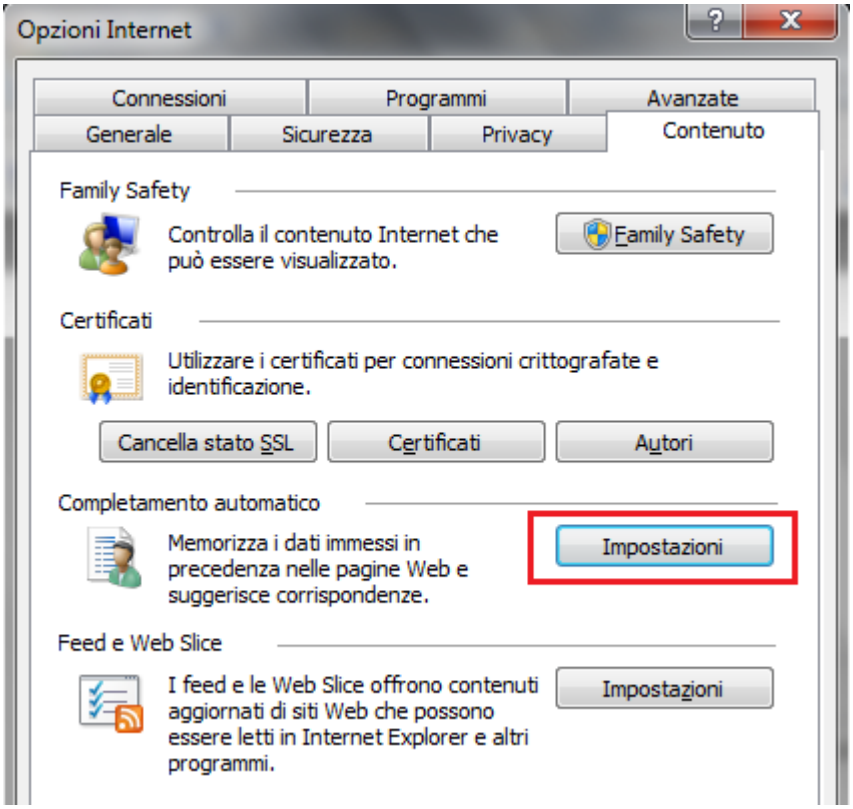
Data la crescente necessità di sicurezza e tutela dei propri dati durante la navigazione in rete, anche gli stessi browser si sono aggiornati, fornendo vari strumenti per tutelare i propri utenti. In questo capitolo facciamo riferimento al browser Internet Explorer 10.

Attivare/disattivare il completamento automatico dei dati

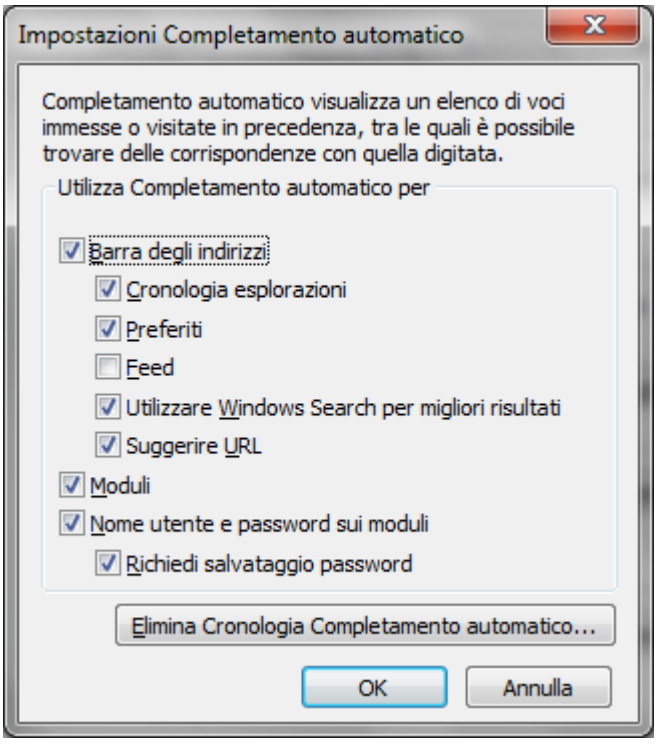
Quando si compila un modulo on line può capitare che il browser completi in modo automatico alcuni campi, proponendo dei valori inseriti in moduli simili o in navigazioni precedenti. È una opzione presente nel browser che gli consente di "ricordare" i dati inseriti e riproporli all'utente. È sicuramente una bella comodità, che evita la riscrittura di informazioni lunghe e complesse come il codice fiscale o il numero di cellulare.
Se il proprio computer è utilizzato da più utenti è conveniente disabilitare queste opzioni di completamento e di salvataggio automatico del browser, per evitare la diffusione dei propri dati personali.
Per disattivare il completamento automatico fare clic su **Strumenti** e scegliere **Opzioni Internet**.



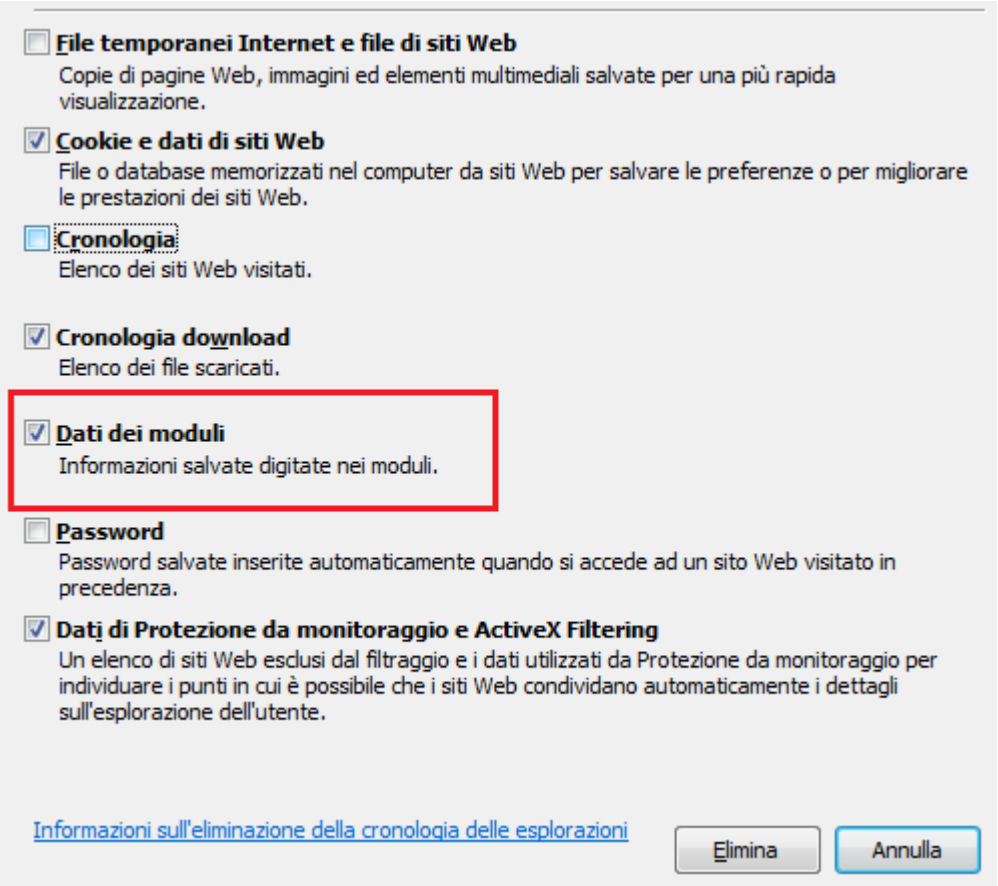
Nella scheda **Contenuto**, nel riquadro Completamento automatico, fare clic su **Impostazioni**.



Appare la finestra per le impostazioni del completamento automatico.



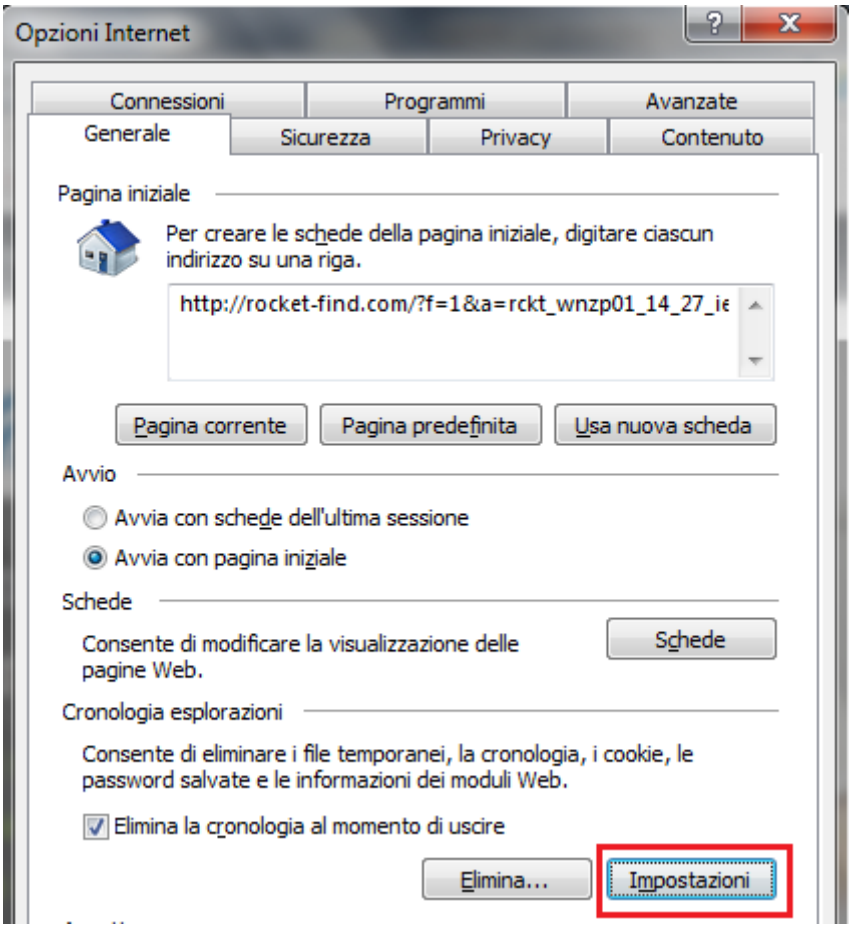
Per disattivare la memorizzazione delle informazioni inserite nei moduli è sufficiente disattivare la rispettiva casella. Per cancellare i dati memorizzati dal browser fare clic su **Elimina Cronologia Completamento automatico**.



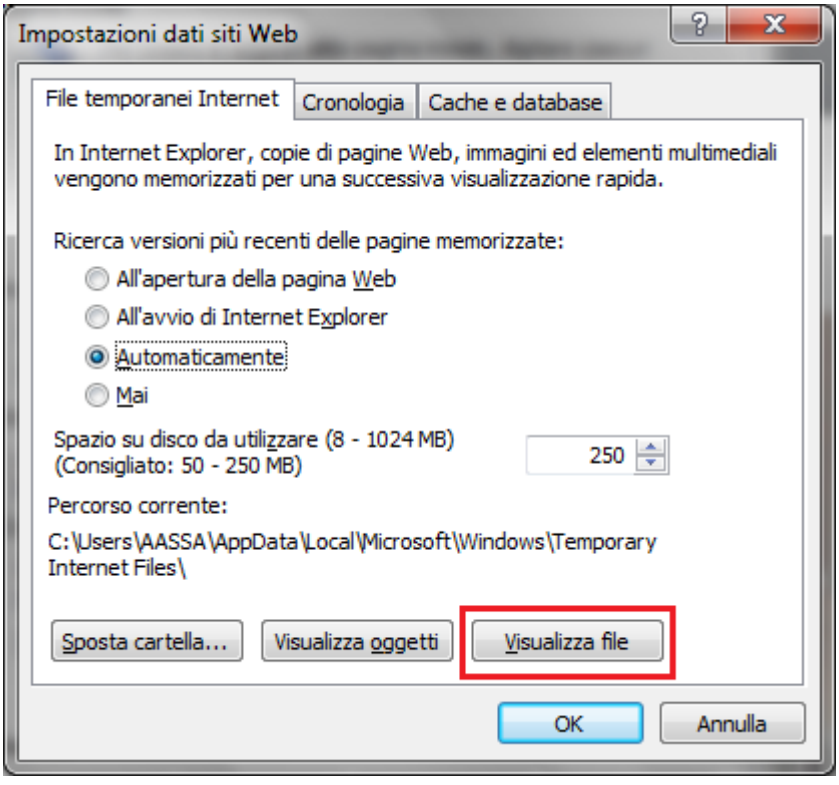
Appare l'elenco delle informazioni che il browser ha memorizzato durante le varie navigazioni. In particolare si possono eliminare i dati scritti nei moduli on line.

I cookie

I **cookie** ("biscotti") sono piccoli file di testo scritti dai siti web tramite il browser con lo scopo di memorizzare alcune informazioni utili a velocizzare un accesso successivo. Ad esempio i dati relativi agli acquisti fatti in un sito, le impostazioni di visualizzazione di una pagina web, ecc. Quando si accede nuovamente alla stessa pagina, il cookie viene inviato dal browser al server per automatizzare la ricostruzione dei propri dati.
L'elenco dei cookie memorizzati è visibile dalla finestra di **Opzioni internet** con un clic sul pulsante **Impostazioni** (scheda **Generale**).

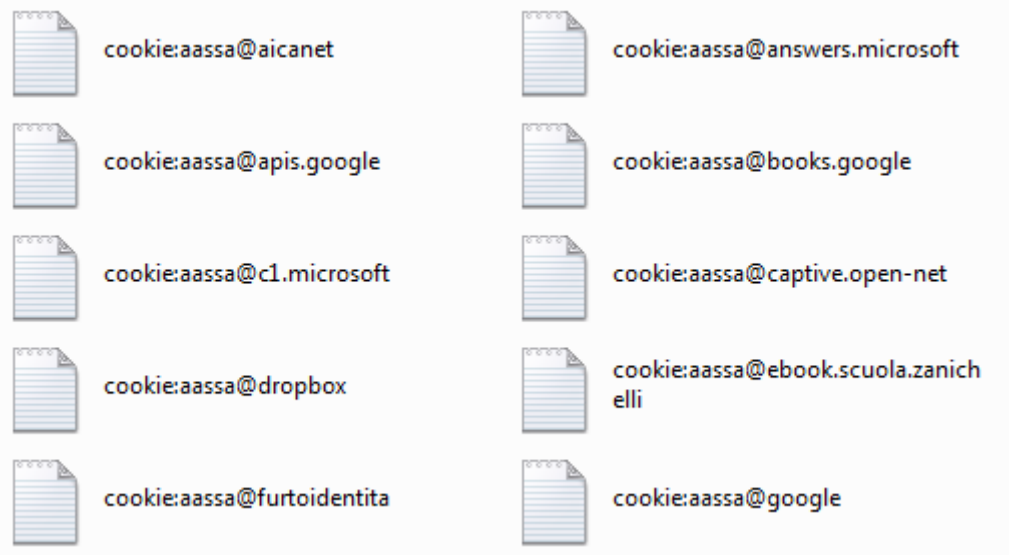


Appare la finestra per le **Impostazioni dati siti Web**.

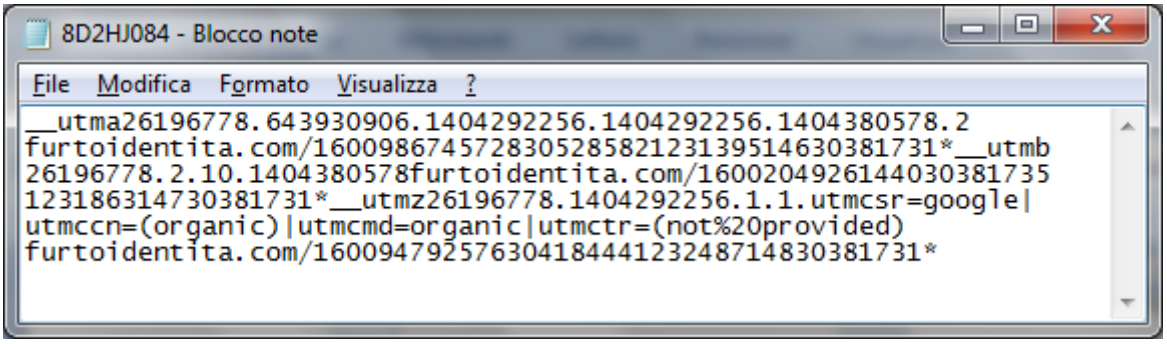


In questa finestra si può impostare come vengono cercate dal browser le versioni più recenti delle pagine memorizzate e quanto spazio del disco rigido viene utilizzato per memorizzare i

cookie e altri file temporanei di internet utili per velocizzare la navigazione. Questi file si possono visualizzare con un clic su **Visualizza file**.



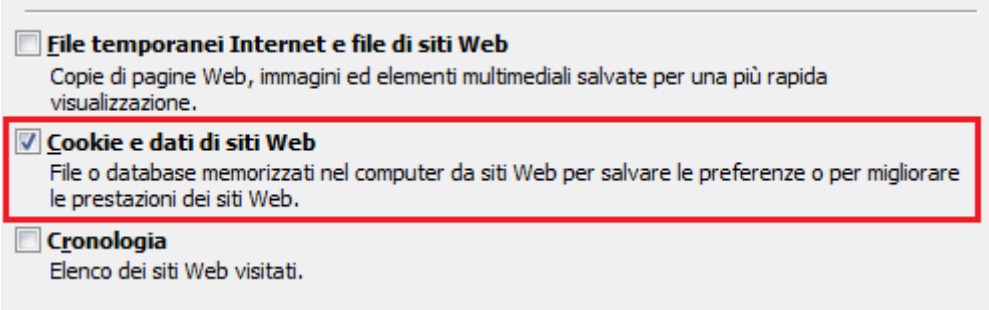
Come abbiamo detto, i cookie sono dei file di testo. Con un doppio clic si possono aprire (appare un messaggio per confermare l'apertura, dato che non sono file scritti dall'utente) e visionare il contenuto.



Il testo è codice per il server del sito, quindi non è comprensibile.
i cookie possono effettivamente contribuire a migliorare l'esplorazione consentendo al sito di raccogliere informazioni utili sulle preferenze dell'utente. Se è utilizzato in modo lecito è uno strumento utile. Ma può capitare che siano usati in modo illecito per tracciare i comportamenti degli utenti, come nel caso degli spyware. Inoltre i cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati.

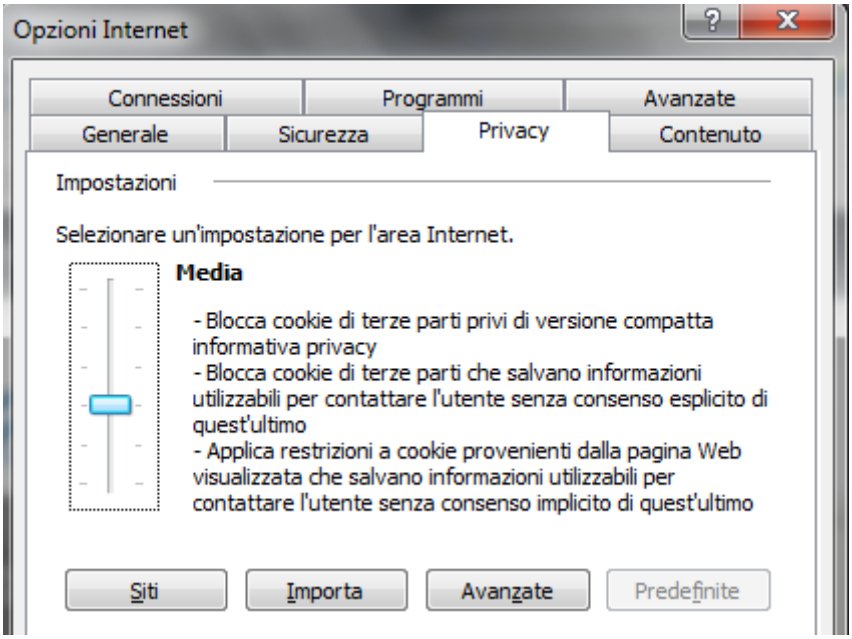
Eliminare i cookie

I cookie memorizzati si possono eliminare premendo il pulsante **Elimina** nella finestra **Opzioni internet** (scheda Generale). Appare l'elenco delle informazioni che il browser ha memorizzato durante le varie navigazioni, visto nel paragrafo precedente. Tra le varie opzioni ci sono anche i cookie.

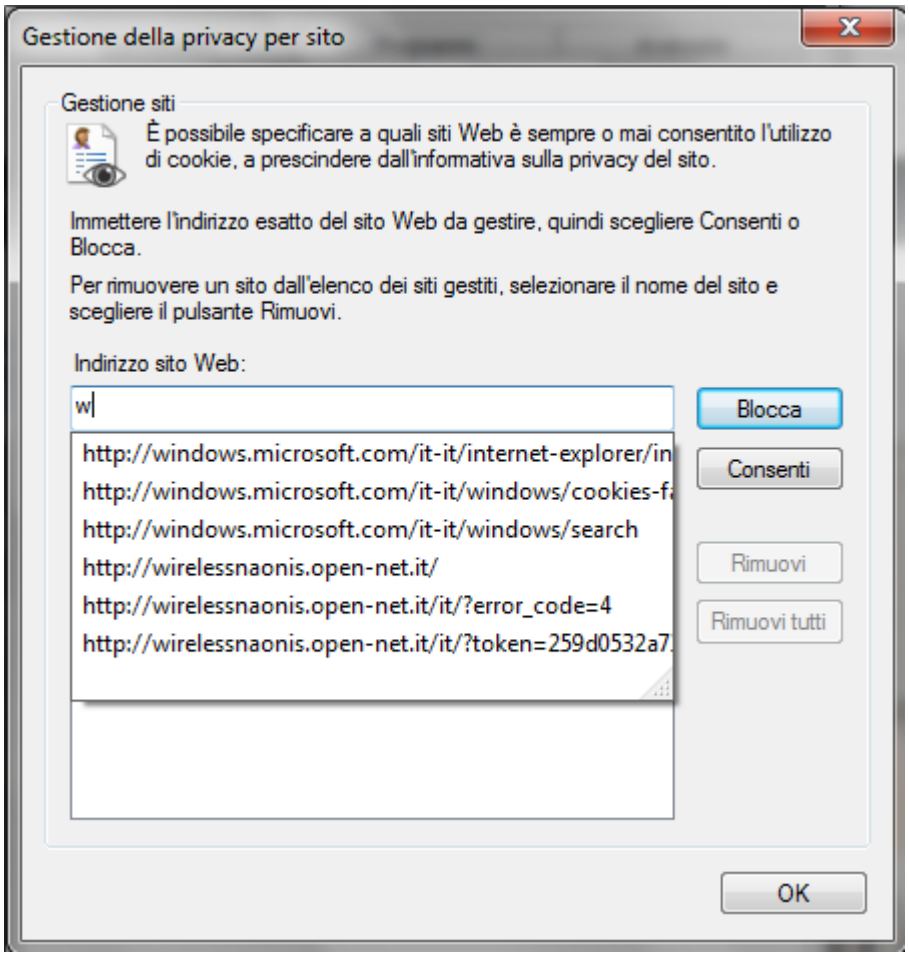


Personalizzare le impostazioni dei cookie

È possibile bloccare o consentire la memorizzazione dei cookie nella scheda **Privacy** della finestra **Opzioni internet**.



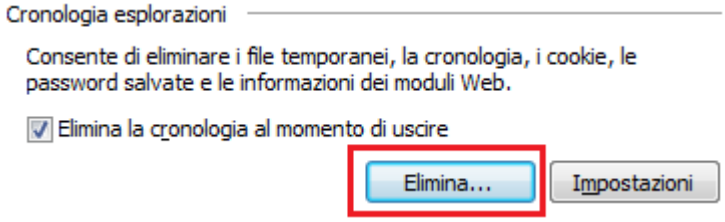
Spostando il dispositivo di scorrimento verso l'alto o verso il basso è possibile specificare tipi generici di cookie considerati accettabili. È ad esempio possibile scegliere di consentire i cookie di siti web che dispongono di informative sulla privacy e bloccare quelli di siti web che memorizzano informazioni personali senza il consenso dell'utente. Se si sposta il dispositivo completamente in alto si bloccano tutti i cookie. Completamente verso il basso si consente qualunque cookie.
Il blocco dei cookie potrebbe impedire la corretta visualizzazione di alcune pagine web.
In alternativa si possono consentire cookie da siti web specifici. Per prima cosa si deve spostare il dispositivo di scorrimento in una posizione intermedia in modo da non bloccare tutti i cookie o non consentirli tutti. Fare clic su **Siti**.



Nella casella **Indirizzo sito Web** digitare un indirizzo di sito web, quindi fare clic su **Blocca** o **Consenti**. Durante la digitazione dell'indirizzo, verrà visualizzato un elenco di pagine web già visitate. È possibile fare clic su una voce dell'elenco, che verrà visualizzata nella casella Indirizzo sito Web.
Ripetere il procedimento per ogni sito che si vuole bloccare o consentire. Al termine, fare clic su **OK** e riportare il dispositivo di scorrimento nella posizione originale.

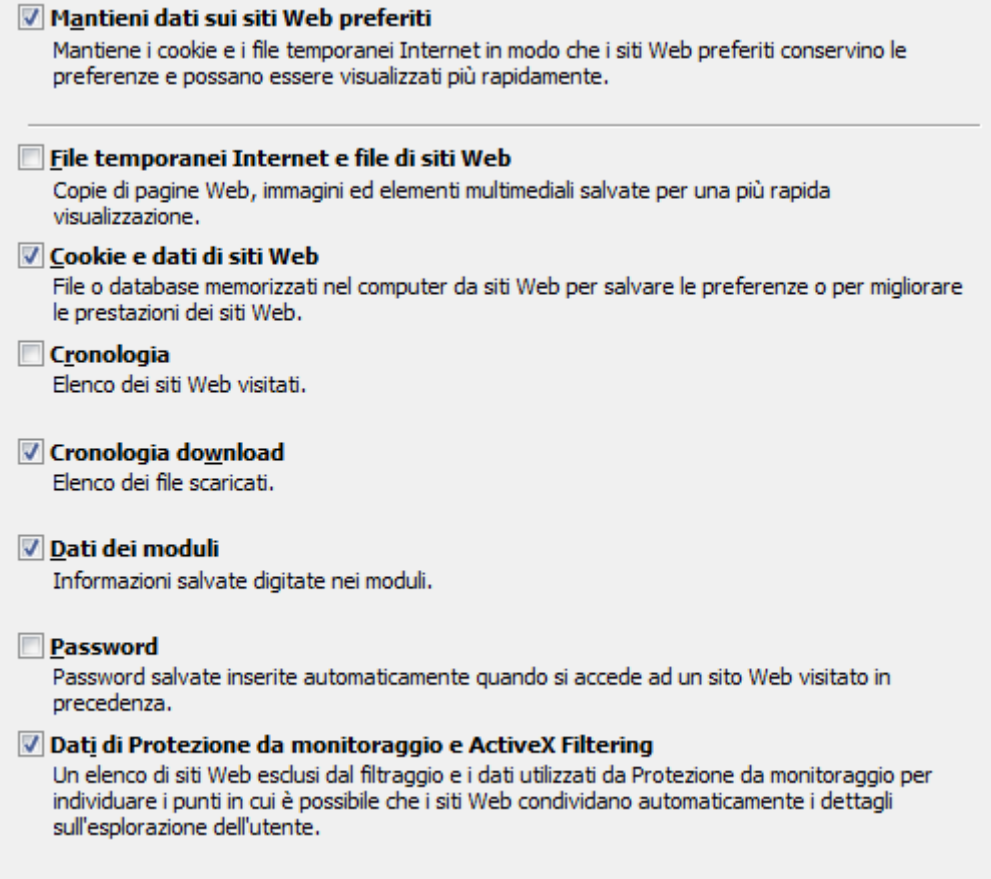
Eliminare i vari dati privati da un browser

Nei paragrafi precedenti abbiamo visto come cancellare le informazioni private che il browser memorizza durante la compilazioni dei moduli.
Dalla stessa finestra è possibile eliminare tutte le altre informazioni personali sulle nostre sessioni di navigazione. Abbiamo visto che si può accedere alla finestra con il pulsante **Elimina** nella finestra **Opzioni internet** (scheda Generale).



In particolare è possibile eliminare i dati della **Cronologia**. La Cronologia contiene i collegamenti relativi ai siti Web visitati nella sessione corrente e nelle sessioni precedenti. In

realtà Internet explorer permette di ripulire questo elenco ogni volta che si chiude la sessione di navigazione con l'opzione **Elimina la cronologia al momento di uscire**.
La finestra **Elimina cronologia esplorazioni** permette di scegliere quali informazioni vogliamo cancellare.



Alcune delle opzioni le abbiamo già viste nei paragrafi precedenti. Le altre sono:

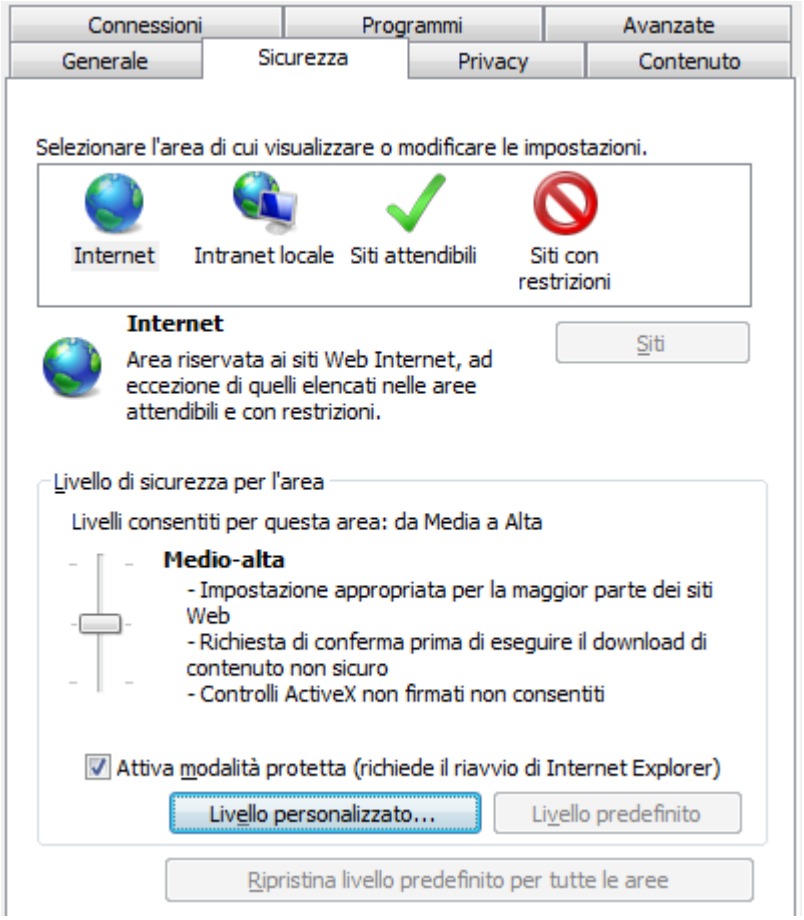
1. **File Internet temporanei**. Sono dei file relativi alle pagine web visitate la prima volta. Sono memorizzate nel computer per velocizzare un accesso successivo a queste pagine.
2. **Cronologia** delle pagine web visitate.
3. **Cronologia download**. Elenco dei file scaricati durante le sessioni di navigazione.
4. **Password** inserite in pagine con accesso protetto.
5. Dati di protezione da monitoraggio e ActiveX Filtering.

Selezionare le informazioni da cancellare e premere **Elimina**.
In particolare, eliminando la Cronologia, si cancellano le voci presenti nell'elenco della Barra degli indirizzi.
In particolare, l'opzione iniziale, **Mantieni dati sui siti web preferiti**, permette di mantenere i cookie e i file associati ai siti presenti nella lista Preferiti.

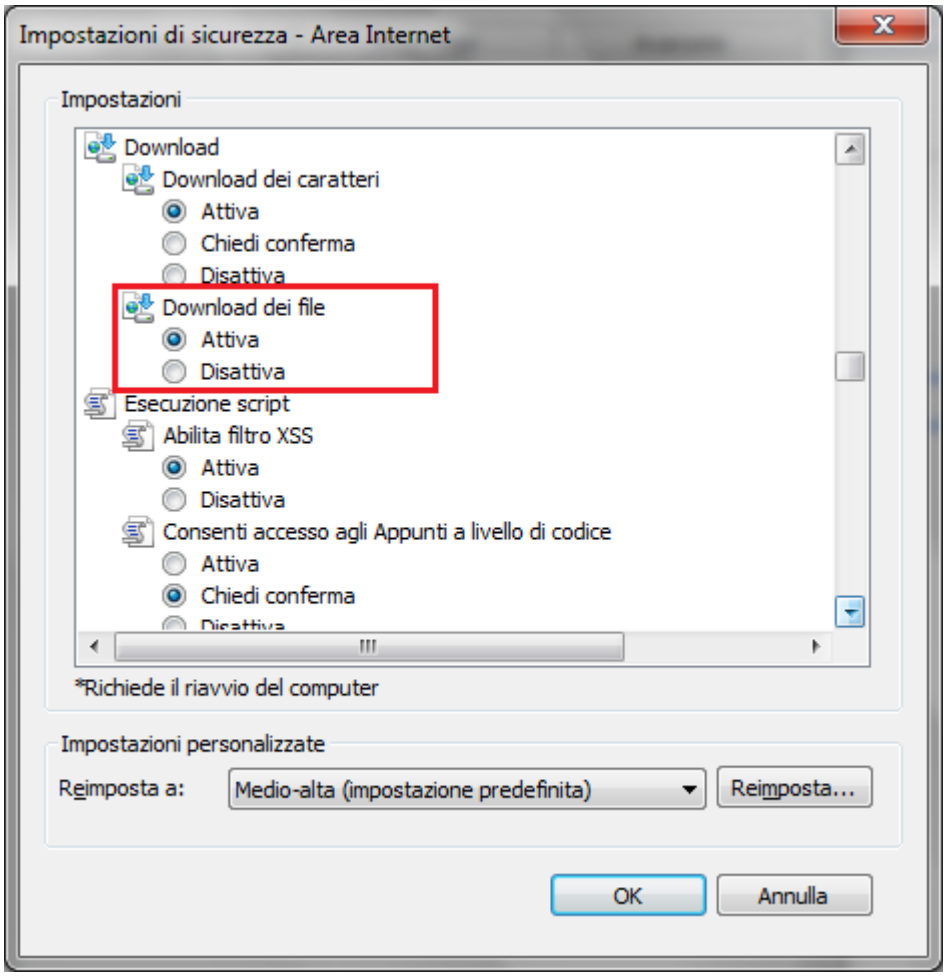
Controllo del contenuto dei siti

In ambito aziendale, esistono software che filtrano l'accesso a internet da parte degli utenti. Ad esempio, per impedire l'accesso a certi siti, come reti sociali, o semplicemente per limitare le operazioni che si possono effettuare in essi (scaricamento di file audio, video, eseguibili, in generale materiale protetto dai diritti d'autore),

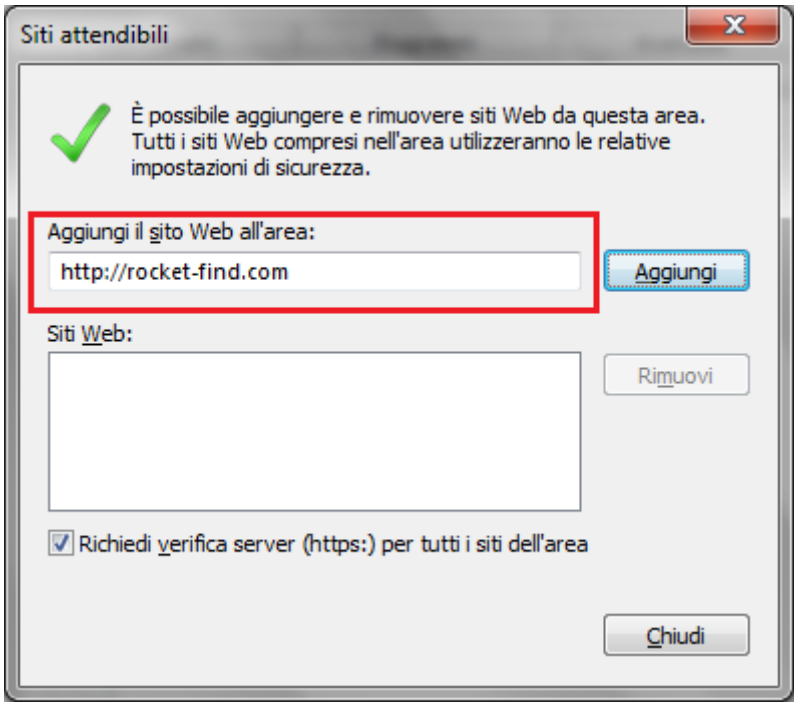
Internet Explorer permette, con la scheda **Sicurezza** in **Opzioni Internet**, di impostare restrizioni alle attività nei siti.



È possibile impostare quattro aree di sicurezza.
Internet: il livello di sicurezza per l'area Internet è applicato a tutti i siti web, ad esclusione di quelli specificati nelle altre aree. Il livello di sicurezza predefinito è Medio alto, ma può essere cambiato in Medio o Alto.
Intranet locale: quest'area riguarda i siti Web e il contenuto archiviato in una rete aziendale. Per i siti di quest'area (e successive) non è applicato il livello di sicurezza indicato nell'area Internet, ma quello dell'area: il livello predefinito è Medio.
Siti attendibili: in quest'area l'utente può indicare i siti che reputa attendibili e non pericolosi per il computer o per le informazioni. Il livello predefinito è Medio.
Siti con restrizioni: qui sono elencati i siti che potrebbero danneggiare il computer o le informazioni. I siti di quest'area non vengono bloccati, ma è impedito l'utilizzo di script o contenuto attivo. Il livello di sicurezza è impostato su Alto e non è modificabile.
È quindi possibile impostare una sicurezza alta ma includere alcuni siti web considerati sicuri ai siti attendibili: oppure, si può impostare una sicurezza bassa e includere siti pericolosi alla lista dei siti con restrizioni.
Per modificare le impostazioni per un'area di sicurezza, si sposta il dispositivo di scorrimento sul livello di sicurezza desiderato.
Si possono creare le impostazioni di sicurezza personalizzate per un'area con il pulsante **Livello personalizzato**. Ad esempio, disabilitare completamente i download.



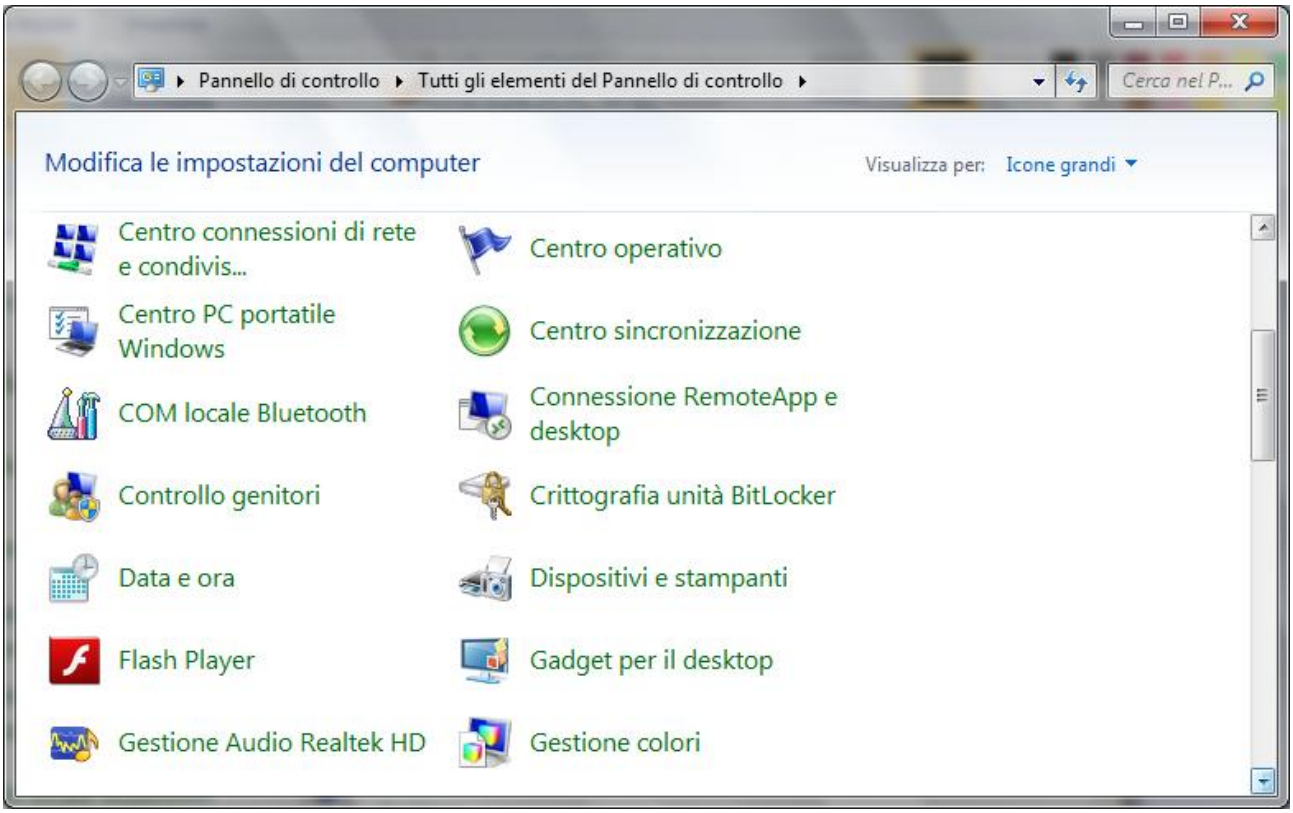
Per ripristinare le impostazioni originali di tutti i livelli di sicurezza, fare clic sul pulsante **Ripristina livello predefinito per tutte le aree**.
Per aggiungere un sito web a un'area di sicurezza, aprire il sito nel browser e selezionare un'area di sicurezza tra Intranet locale, Siti attendibili e Siti con restrizioni. Fare clic su **Siti**. Il sito Web verrà visualizzato nel campo **Aggiungi il sito Web all'area**.



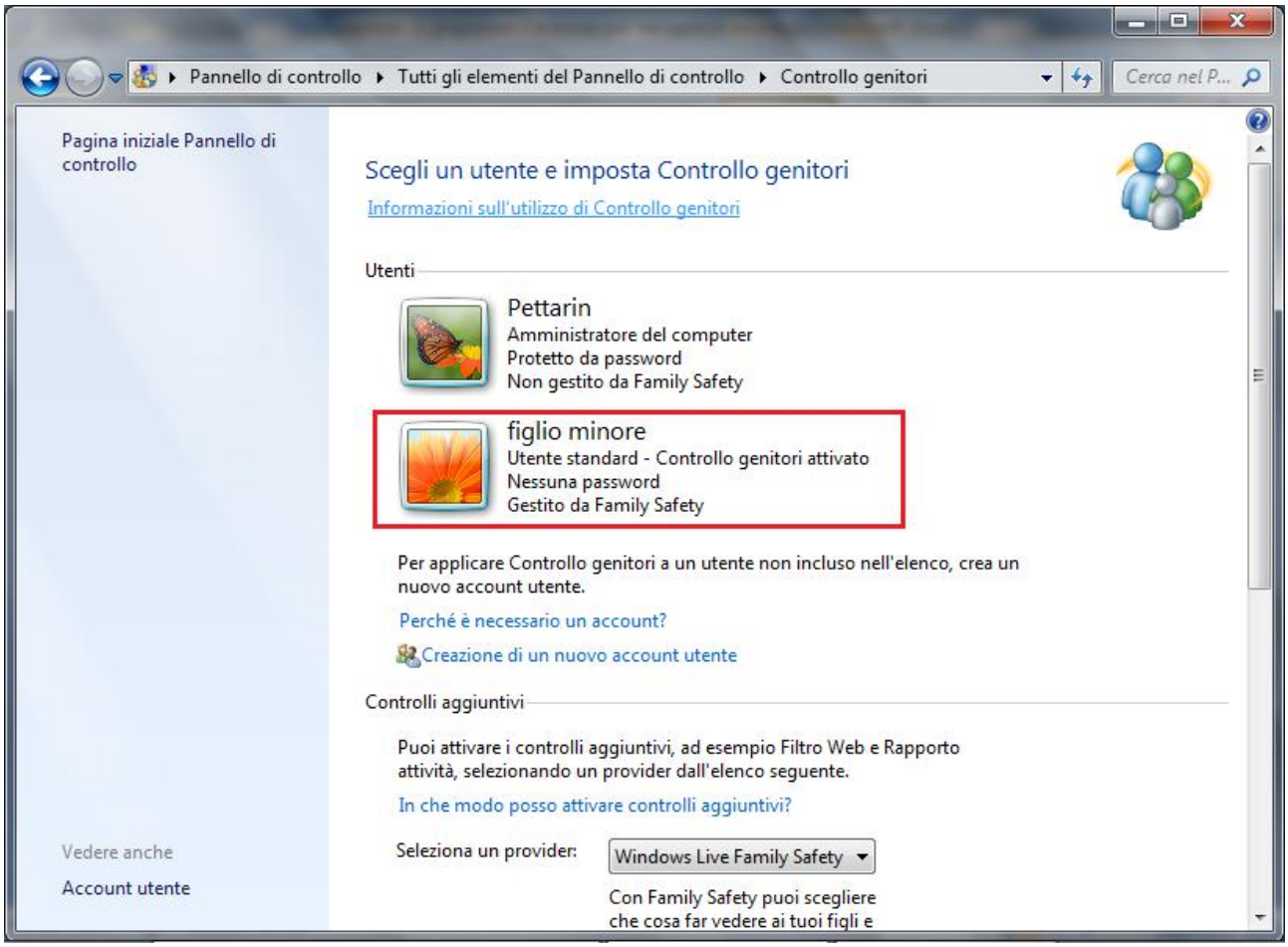
Fare clic su **Aggiungi**. Per rimuovere un sito web da un'area di sicurezza, la procedura è simile. è sufficiente fare clic su **Rimuovi**.

Controllo genitori

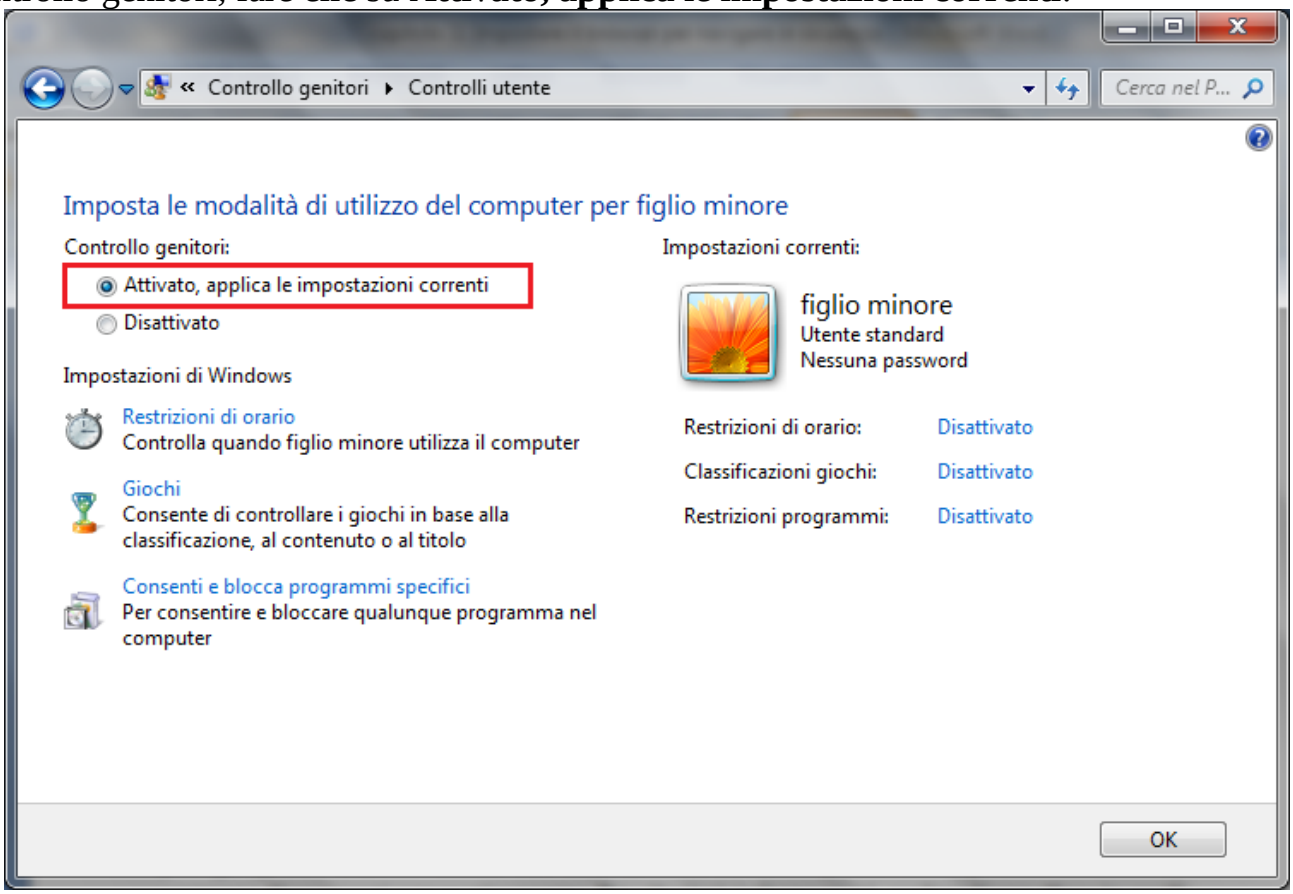
Con Windows 7 si possono impostare delle restrizioni che limitino l'uso del computer e di internet ad alcuni utenti, ad esempio i minori.
Nel Pannello di controllo, il programma **Controllo genitori** permette di impostare il tempo di utilizzo del computer da parte di un utente e specificare i programmi e i giochi che può utilizzare.



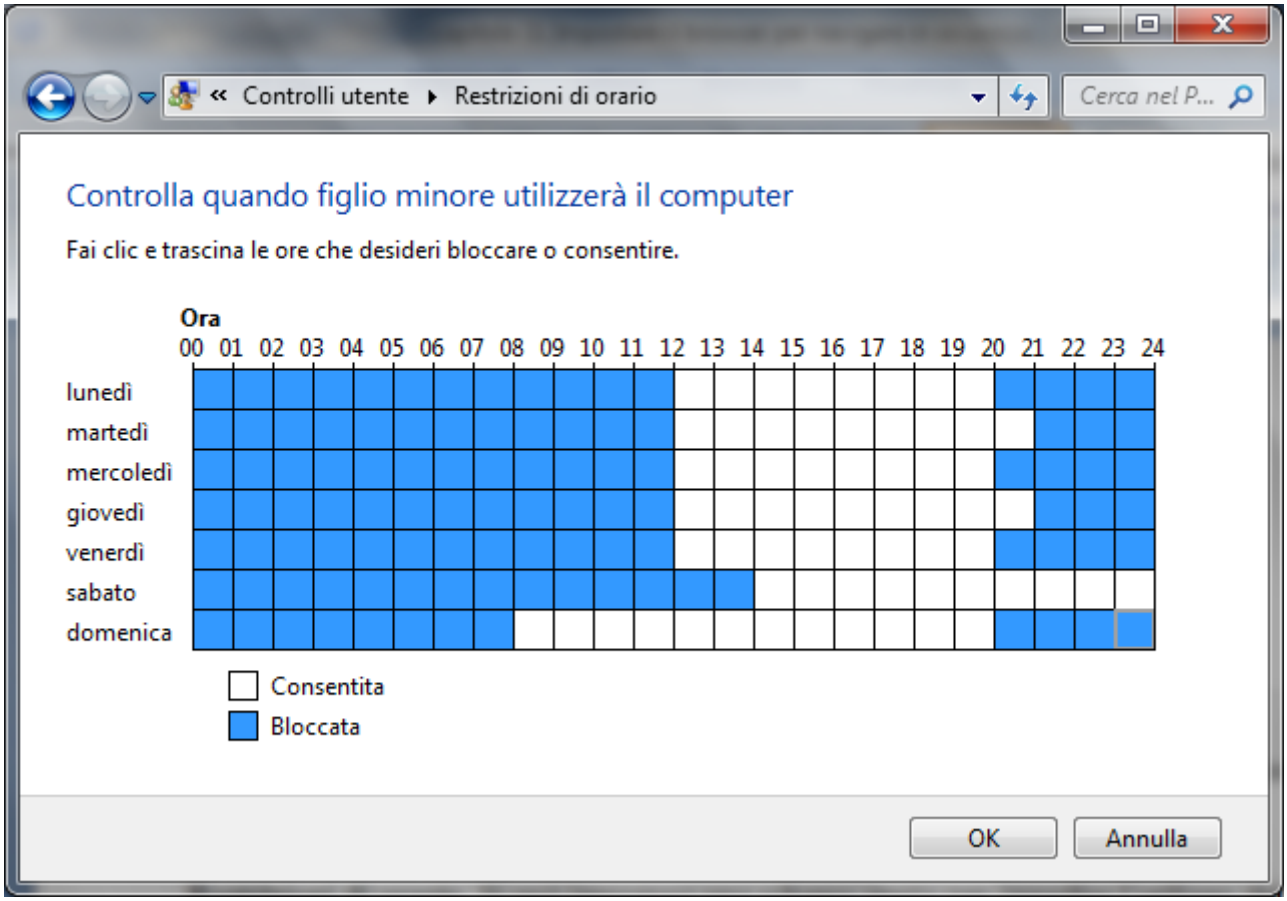
Per impostare il Controllo genitori su un utente si deve accedere come amministratore o fornire una password amministratore.



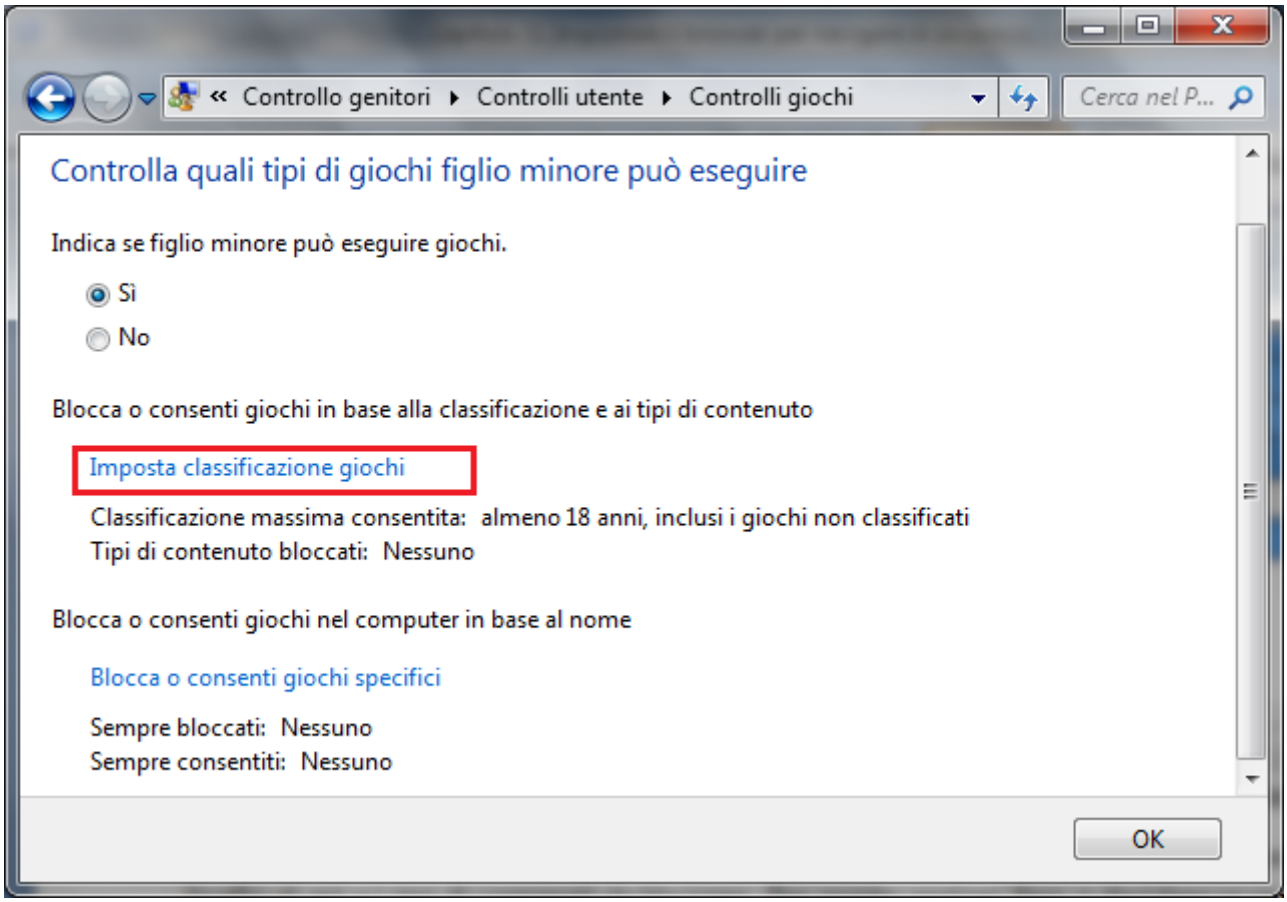
Scegliere l'account utente standard per il quale configurare Controllo genitori. Nella finestra Controllo genitori, fare clic su **Attivato, applica le impostazioni correnti**.



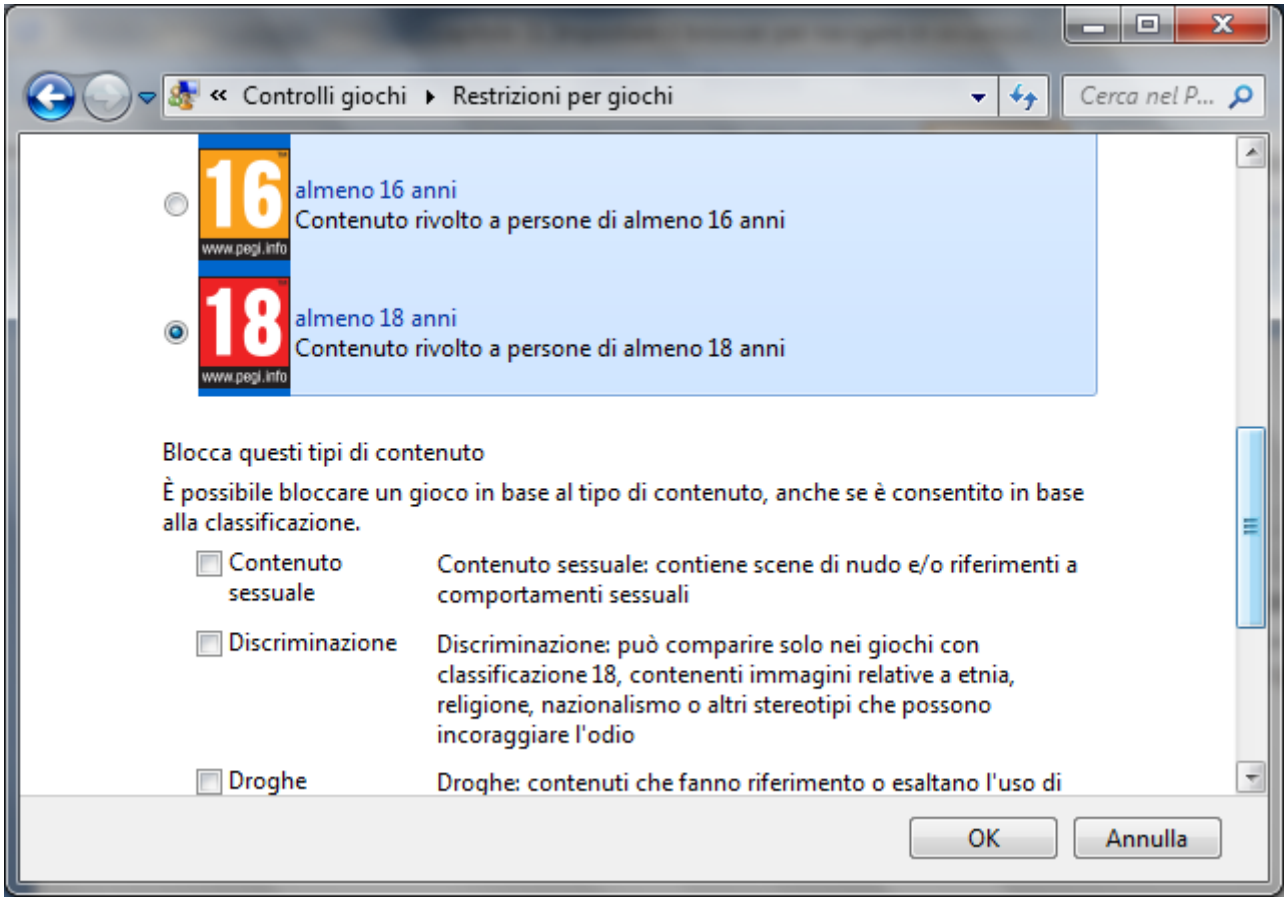
A questo punto si possono modificare le specifiche restrizioni.
Restrizioni di orario. Si può impostare uno schema orario per impedire l'utilizzo del computer nelle ore specificate, anche con orari diversi per ogni giorno della settimana.



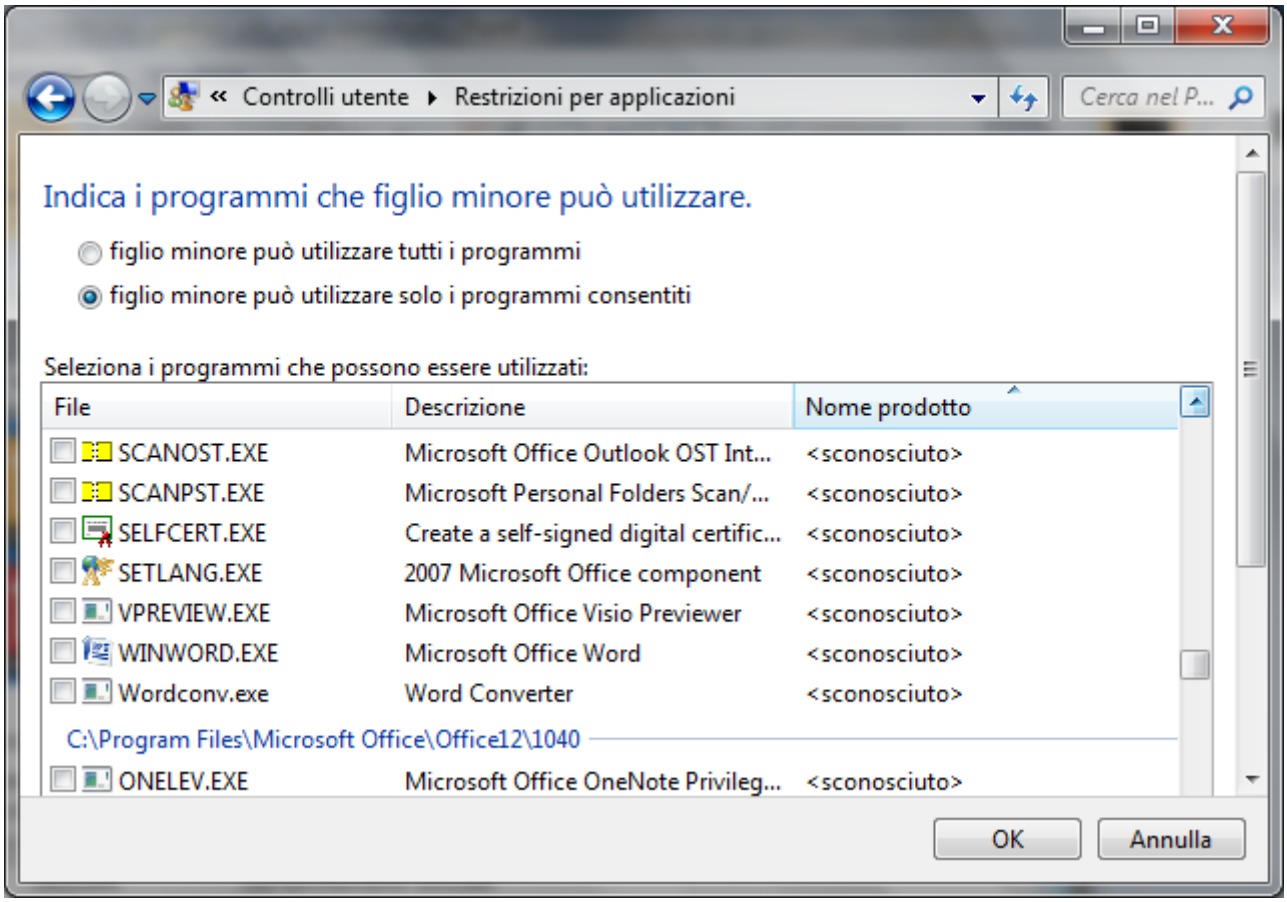
Giochi. Si può specificare quali giochi può eseguire l'utente.



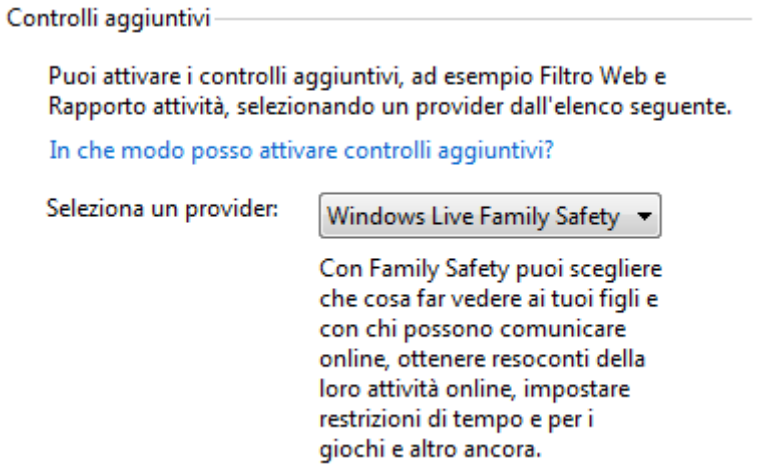
In particolare si può specificare un livello di età e i tipi di contenuti da bloccare. Per queste opzioni fare clic su **Imposta classificazione giochi**.



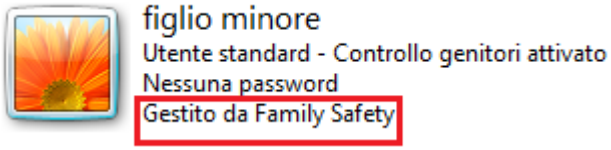
È poi possibile bloccare o consentire l'utilizzo di giochi specifici, con il comando **Blocca o consenti giochi specifici**. In modo simile è possibile
consentire o bloccare programmi specifici. Si può impedire l'utilizzo di determinati programmi con un clic sul comando **Consenti o blocca comandi specifici**.



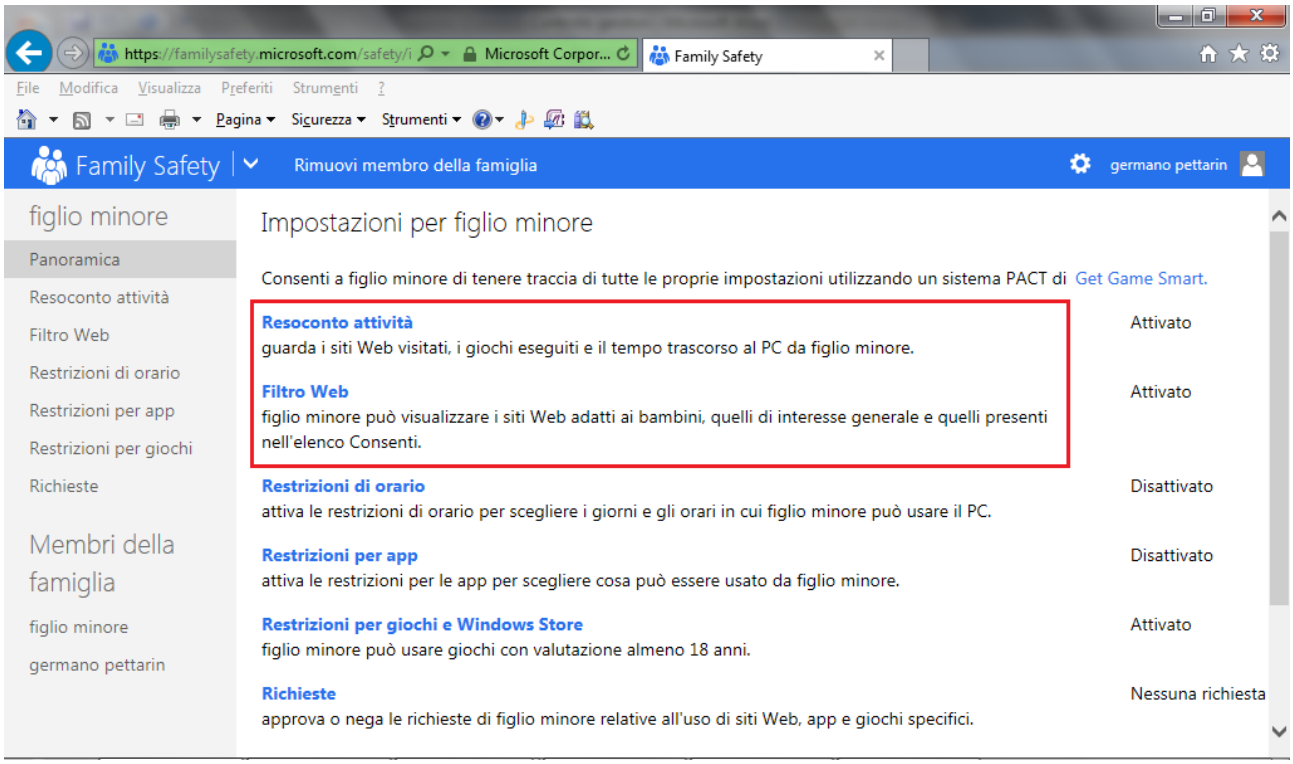
Oltre ai controlli di base inclusi in Windows, è possibile installare controlli aggiuntivi di altri provider di servizi che possono essere utilizzati in Controllo genitori, ad esempio, restrizioni per i siti Web e il resoconto attività.
Se questi controlli aggiuntivi sono già presenti nel computer appare il nome del provider nel menu del riquadro **Controlli aggiuntivi** di Controllo genitori.



Nel nostro caso è stato scelto Windows Live Family Safety. È un componente di Windows Essentials disponibile gratuitamente. Con Family Safety si può configurare il filtro Web e il resoconto attività.
Una volta selezionato il provider, tutte le funzioni del Controllo genitori, per l'utente in questione, è gestito dal sito di Family Safety.



Con un clic sull'icona dell'account si accede alla pagina di configurazione dei controlli di Family Safety.



Oltre alle opzioni già viste per Controllo genitori c'è la possibilità di filtrare i siti e di ottenere un resoconto sui siti web visitati, i giochi eseguiti e il tempo trascorso al computer.