icar ONLUS

ce l'ha fatta!

www.associazioneicaro.org

Non solo rischi…

Controllo a distanza
- Videocamera
- Geolocalizzazione
- Traffico dati
- Contenuto messaggi

Danni alla reputazione
- Immagini
- Commenti
- Like (es. Graphsearch)

Minacce materiali
- Adescamento on-line
- Cyberbullismo
- Frodi finanziarie
- Ransomware
- Furto di beni

Perdita di controllo delle mie informazioni
- Furto di dati
- Condivisione App
- Diffusione Ingenua

Cybercrime
- Botnet per attacchi
- Furto identità digitale per frodi
- Traffico super-costoso

icaro ce l'ha fatta!
www.associazioneicaro.org

..ma anche opportunità

Come vivere al meglio la rete..

icaro ONLUS
ce l'ha fatta!
www.associazioneicaro.org

Tecnologia più sicura

- Prodotti
- "Settings"
- Servizi

Comportamenti consapevoli

- Conoscenza
- Esperienza
- Apprendimento
- Confronto

Problem Exist Between Keyboard And Chair

..seguendo un percorso di crescita continua

Accettazione del rischio
(conoscenza dei limiti)

Richiede l'esperienza che gli adulti stanno ora consolidando nel mondo virtuale

Contromisure
(conoscenza dei rischi)

Efficacia limitata nel tempo e all'evoluzione tecnologica

Percorso educativo

- Sensibilizzazione ragazzi
- Formazione genitori e insegnanti
- Laboratori emotivi
- Conoscenza della netiquette
- Massimizzazione degli strumenti

Smart-habit
(consolidamento nella vita quotidiana dei concetti acquisiti e loro condivisione tramite esempio)

Teatro, video, scritture, testimonianze, …

Alcuni comportamenti furbi..

Password sicura!

la password dovrebbe essere lunga almeno 8 caratteri e composta sia di lettere che di numeri e non riconducibile a informazioni facilmente collegabili alla nostra persona (es. data di nascita o matrimonio, …); non riveliamo a nessuno la nostra password (unica eccezione la password dei bambini più piccoli che deve essere condivisa con i genitori) e non scriviamola nella rubrica del cellulare o nel quaderno degli appunti che teniamo di fianco al pc; utilizziamo password diverse tra un sito e l'altro e tra il router e la rete wireless domestica; ricordiamoci che sul web si trovano facilmente e gratuitamente programmi che ci possono aiutare generando password complesse e archiviandole in modalità sicura sul nostro pc o il nostro smartphone

..ma non solo: domanda di riserva sicura!

chi cerca di entrare nel nostro account può utilizzare il link "Hai dimenticato la password?"; spesso le risposte a queste domande sono rintracciabili nei contenuti che abbiamo postato sul web – es. nome del cane, scuola frequentata, marca di birra preferita…

Postiamo con la testa!

consideriamo sempre che tutto quello che inseriamo nei social network può essere "per sempre": anche se eliminassimo il nostro account i nostri amici hanno avuto la possibilità nel tempo di scaricare, salvare o condividere i nostri commenti o le nostre foto; ricordiamoci poi che la cancellazione definitiva del dato è un'operazione difficile e costosa, tanto che per i provider di servizi garantirne la reale esecuzione è al limite dell'impossibile

Amicizie selettive!

nell'accettare o nel cercare amicizia sui social network, ricordiamoci del "numero di Dunbar": è impossibile avere centinaia e centinaia di veri amici; pensiamo sempre se al potenziale amico vorremmo dare davvero tutte le informazioni che postiamo sul web

Dubitiamo del mittente!

evitiamo di dare per scontato che i messaggi siano veramente inviati dal nome che ci appare; quando sospettiamo che un messaggio sia fraudolento, cerchiamo un metodo alternativo per contattare il mittente e verificare la provenienza del messaggio o dell'invito ad un nuovo social network

Clikkiamo con attenzione!

trattiamo i link che riceviamo dai nostri amici sui social network allo stesso modo di quelli contenuti nelle e-mail; facciamo attenzione ai messaggi di vincite straordinarie o incredibile fortuna: spesso celano sorprese spiacevoli

Digitare è meglio che clikkare!

raggiungiamo le nostre pagine personali digitando direttamente l'indirizzo del social network nel browser o usando i segnalibri personali: fare click su un link ci espone al rischio di immettere nome e password dell'account in un sito falso, è quello che si chiama "phishing"

icaro ONLUS
ce l'ha fatta!
www.associazioneicaro.org

..utili in qualsiasi occasione

Attenzione alle trappole!

a volte possiamo essere vittime di attacchi che sfruttano le nostre paure e la nostra buona fede: evitiamo di scaricare (download) programmi che non riconosciamo a seguito di pop up o messaggi anche se affermano di proteggere il nostro PC o di rimuovere virus individuati sulla nostra macchina, è molto probabile che facciano l'esatto contrario; in generale cerchiamo di scaricare software esclusivamente da siti affidabili e diffidiamo delle offerte gratuite di musica, giochi, video e premi; usiamo cautela nell'aprire allegati o fare clic su link contenuti nelle email, riportati in chat, postati sui social network o riportati nei banner pubblicitari (evitiamo quindi di clikkare su "Avanti", "OK" o "Accetto"): se abbiamo dei dubbi chiudiamo il browser chiudendo, alla relativa richiesta, tutte le schede senza salvarle per il successivo riavvio del browser.

Pesiamo le App!

valutiamo bene le "App" che scarichiamo sulla nostra pagina social o sui nostri smartphone: spesso le app possono accedono senza che ce ne accorgiamo alle informazioni del nostro pc, tablet o smartphone; quando diamo l'ok al download leggiamo in fondo al disclaimer le tipologie di dati cui le app richiedono l'accesso e valutiamo se ciò sia realmente necessario

Scegliamo noi la nuvola!

analizziamo bene i siti su cui salviamo periodicamente i nostri dati: il salvataggio remoto mediante tecnologia "cloud" può essere più comodo e semplice della copia su disco fisso esterno; non tutti i siti però forniscono i medesimi livelli di sicurezza, quali ad esempio la protezione (cifratura) del canale con cui si caricano e scaricano i dati

icaro ONLUS
ce l'ha fatta!
www.associazioneicaro.org

Chiudiamo a chiave il wi-fi!

le connessioni non protette sono una facile sorgente di informazioni gratuite: proteggiamo la nostra rete con le chiavi di sicurezza e diffidiamo delle reti libere che troviamo per strada

Antivirus forever!

usiamo e aggiorniamo l'antivirus sia sui pc che sugli smartphone: virus, worm e trojan sono programmi insidiosi che possono manipolare il nostro computer e i spiare o anche cancellare i dati memorizzati; impostiamo aggiornamenti automatici e scansioni continue e periodiche - sebbene a volte possa sembrare che questo causi rallentamenti o perdite di tempo: l'antivirus è il primo livello di protezione dei nostri strumenti, come le guardie sugli spalti del nostro castello

Proteggiamoci con il Firewall!

il firewall è un programma, spesso integrato nel sistema operativo o negli antivirus, che lascia passare sia in entrata che in uscita solamente i dati che hanno il nostro permesso: attiviamolo; il firewall è come le mura del nostro castello

Software sempre aggiornato!

quando i produttori scoprono un punto debole nel loro software pubblicano un update (o patch) per impedire che gli hacker possano sfruttare questa falla: acconsentiamo alle richieste di update, sembra una noia ma non lo è

..utili per una navigazione "social-MENTE" attiva

icaro ONLUS
ce l'ha fatta!
www.associazioneicaro.org

Impariamo a conoscere i Social network!

scegliamo i social network con attenzione e leggiamone l'informativa sulla privacy: possiamo scoprire cose interessanti e curiose sulle modalità con cui questi siti trattano i nostri dati

Un solo amministratore per tutti, un'utenza per ognuno!

Sul pc, preferiamo lavorare con utenze che non abbiano diritti di amministratore, chi ci "ruba" l'utenza eredita i diritti ad essa connessi – ad esempio, se prendiamo un virus quando siamo connessi come amministratori, questo virus avrà i diritti di amministratore sulla nostra macchina; se il pc o il tablet sono condivisi, creiamo un utenza per ognuna delle persone che ci accedono: anche questo diminuisce il rischio di perdita dei dati e permette livelli di protezione più precisi

Impostiamo correttamente i livelli di privacy dei browser!

tutti i browser danno la possibilità di alzare o abbassare i livelli di protezione della privacy: a livelli più alti corrispondono funzionalità più limitate e viceversa, è quindi importante trovare il giusto equilibrio per ogni utente (ad esempio più alto per i ragazzi, minore per gli adulti); le modalità di impostazione variano da prodotto a prodotto ma possono essere facilmente trovate curiosando un po' nei menù a tendina

Navighiamo in sicurezza!

impostiamo la sicurezza di google e di youtube al massimo livello per ridurre la possibilità che, per errore, durante la navigazione ci si imbatta in immagini e video non adatti o sgradevoli; blocchiamo poi la visualizzazione delle finestre popup utilizzando le funzionalità di blocco integrati nei browser;

Mettiamoci in gioco!

parliamo con i nostri ragazzi della loro e della nostra vita sul web, mostriamo interesse verso le loro attività online e discutiamo dei problemi ma anche delle numerosissime e divertenti cose che è possibile fare con il Web; impariamo anche noi ad utilizzare maggiormente Internet e chiediamo ai nostri ragazzi consigli sull'utilizzo dei diversi strumenti strumenti: ammettere i nostri limiti tecnologici può aiutare a creare un momento di condivisione senza perdere il ruolo di educatore; discutiamo con loro di ciò che è più opportuno fare in caso di situazioni sgradevoli anche se queste non si sono mai avverate

Navighiamo insieme ai ragazzi!

creiamoci delle occasioni per navigare insieme ai ragazzi: ad esempio pianifichiamo insieme un viaggio, cerchiamo siti relativi ai loro hobby: navigando insieme possiamo aiutare i nostri ragazzi a valutare il valore delle informazioni trovate

..utili contro il cyberbullismo

1. "Don't feed the trolls": evitare di reagire, evitare di rispondere ai cyberbulli.
2. Usicre dal web per trovare la soluzione: annotare e stampare quello che disturba e parlarne con chi può aiutare (genitori, insegnanti, educatori, operatori di numero verde..)
3. Non partecipare al bullismo, il "like" rende complice (e vittima)
4. Frequentare i social con uno scopo, non andare "in piazza" a perdere tempo, il web offre tante altre possibilità più divertenti
5. Proteggersi evitando di fornire informazioni o immagini personali e private
6. Praticare uno sport (:o) – si litiga, ci si sfoga, ci si diverte rimanendo in una dimensione reale

Cosa possiamo fare per aiutare i nostri ragazzi..

1. più sono piccoli più cerchiamo di **essere presenti** quando i ragazzi usano Internet;
2. stabiliamo delle **regole precise** per l'utilizzo di Internet (tempi, modi, …);
3. raccomandiamogli di **non condividere informazioni personali** come nome, indirizzo, numero di telefono o password con gli altri utenti di Internet; le foto e altre informazioni private non dovrebbero mai essere condivise con utenti che si conoscono solo online;
4. facciamogli capire che è corretto **condividere sul web foto, immagini e informazioni dei propri amici solo con il loro consenso**
5. quando ci chiedono di attivare il loro primo account sui social network **facciamoci dare la loro amicizia**: più che un controllo è un modo semplice di aiutarli e dar dei consigli sul loro comportamento; ricordiamoci che per registrarsi in facebook è necessario aver compiuto almeno i 13 anni;
6. quando costretto a registrarsi sui siti, magari per giocare, aiutiamolo a crearsi **un'utenza che non riveli alcuna informazione personale** – soprattutto età o sesso; nel form di registrazione indichiamo l'indirizzo mail di un adulto;
7. usiamo gli strumenti di "**parental control**" per creare profili appropriati e filtrare i contenuti di Internet, ma ricordiamoci che **questi strumenti sono solo un aiuto ma non sono sufficienti a proteggerlo;**
8. incoraggiamoli **a spiegarci se qualcosa o qualcuno in Internet li fa sentire a disagio** o minacciati: facciamogli capire che se hanno dei dubbi siamo a loro disposizione per parlarne subito;
9. ricordiamogli che è meglio che **interrompano subito** qualunque comunicazione (via e-mail, chat, instant messaging) se qualcuno inizia a rivolgere loro domande troppo personali o dal contenuto sessuale;
9. suggeriamogli di **"chattare" nell'area pubblica** evitando le chat private dove non è possibile monitorare le conversazioni (aree "whisper"); suggeriamogli anche di evitare di rivelare nelle chat o nei forum informazioni personali (tra cui età e sesso) o informazioni sulla famiglia;
10. usiamo noi internet in sicurezza consapevoli di essere un **modello di riferimento** per i più piccoli;
11. diamo **priorità alle loro richieste** e al loro desiderio di parlarci della loro vita in rete: le altre nostre attività possono aspettare;
12. informiamoci sui **siti Web visitati dai nostri ragazzi** e sugli utenti con cui parlano;
13. insistiamo sul concetto che non debbano **mai incontrare di persona da soli un amico conosciuto online**, e poi insistiamo ancora; nel caso, accompagniamoli noi o – nel peggiore dei casi - assicuriamoci che vadano all'incontro accompagnati da amici; l'incontro deve sempre avvenire in un luogo pubblico;
14. insegniamo ai ragazzi a **scaricare** programmi, musica o file **solo con l'autorizzazione di un adulto** (la condivisione e l'utilizzo di file può essere illegale);
15. parliamo con i nostri ragazzi adolescenti dei contenuti online per adulti e della pornografia: indirizziamoli verso **siti adatti, dedicati alla salute e alla sessualità;**

icaro ONLUS
ce l'ha fatta!
www.associazioneicaro.org

..senza aver paura di metterci in gioco

17. aiutiamoli a proteggersi dallo spam: raccomandiamogli di non condividere il proprio indirizzo e-mail online e di **non rispondere alla posta indesiderata;**
18. valorizziamo, anche con il nostro comportamento e linguaggio, un **comportamento online etico e responsabile**; facciamo in modo che non utilizzino Internet per diffondere pettegolezzi, rendersi protagonisti di cyber-bullismo, insultare, offendere o minacciare altri utenti;
19. parliamo con loro anche del **gioco d'azzardo online** e dei potenziali rischi di questa attività: tra l'altro il gioco d'azzardo dei minorenni – anche online - è illegale
20. condividiamo con loro che **"crakkare", "jailbrekkare" e "roottare" i sistemi dei pc e degli smartphone (in pratica manomettere i sistemi operativi per poter fare più cose) non è una buona idea:** si perde la garanzia sull'acquisto e aumenta la possibilità di essere attaccati dai virus

Come con la posta normale, usiamo anche una casella postale di famiglia!

creiamo un indirizzo di posta elettronica per tutta la famiglia per registrarsi sul web, creare profili, fare acquisti in Internet e altre attività simili: in questo modo possiamo proteggere il nostro indirizzo di posta elettronica personale prevenendo anche lo spam; aspettiamo a creare indirizzi di posta elettronica personali per i nostri ragazzi quando sono troppo piccoli

Agiamo con fermezza!

qualora venissimo a conoscenza che i nostri ragazzi abbiano ricevuto da un contatto online foto o richieste dal contenuto sessuale esplicito, rivolgiamoci immediatamente alla polizia. Conserviamo tutta l'eventuale documentazione, tra cui indirizzi e-mail, indirizzi di siti Web e registri delle chat

Sentiamoci pronti

parliamo con i nostri ragazzi della loro vita on line con le stesse modalità con cui parliamo normalmente della loro vita reale (amici, attività, delusioni, …);

Alcuni siti che ci possono aiutare a capire meglio

icaro ONLUS
ce l'ha fatta!
www.associazioneicaro.org

Informazione e strumenti

- www.disney.it/CyberNetiquette
- www.ecpat.it
- www.gianofamily.org/
- www.google.it/goodtoknow/familysafety/
- www.navigaresicuri.telecomitalia.it
- www.noncaderenellarete.it
- www.saferinternetday.org
- www.savethechildren.it/italia/nuove_tecnologie.html
- www.security4kids.ch/?lang=it-CH
- www.swisscom.ch/it/ghq/responsabilita/comunicazione-per-tutti/tutela-dei-giovani-dai-media
- www4.ti.ch/can/ragazzi-e-internet
- http://www.cyberbullying.org (in inglese)
- http://www.citta-invisibile.it

Istituzionali

- www.garanteprivacy.it/connettilatesta
- www.poliziadistato.it/articolo/1106/

Game

- www.netcity.org
- www.wildwebwoods.org

link ad altri siti interessanti

- www.dienneti.it/bambini/internet-sicuro.htm

Alcuni antivirus gratuiti

- **Microsoft**
  www.microsoft.com/security_essentials
- **Avast! Software**
  www.avast.it
- **AVG Technologies**
  www.free.avg.com/it
- **AVIRA**
  www.free-av.com/It
- **SOPHOS**
  www.sophos.com (solo per MAC)

Alcuni antivirus a pagamento

- **BITDEFENDER** www.bitdefender.it
- **ESET** www.nod32.it
- **AVIRA** www.avira.com/it
- **SYMANTEC** www.symantec.com/it
- **G DATA** www.gdata.it
- **KASPERSKY** www.kaspersky.com/it
- **AVG TECHN.** www.avg.it
- **AVAST** www.avast.com/it-it
- **SUN BELT** www.sunbeltsoftware.com
- **F-SECURE** www.f-secure.com/it_IT
- **TREND MICRO** it.trendmicro.com
- **PANDA** www.pandasecurity.com
- **AGNITUM** www.agnitum.com
- **MCAFEE** www.mcafee.com/it

Un esempio per gestire le password

- Non mettere la stessa password ovunque
- Scegli password difficili da indovinare
- Per ricordare le password utilizza software che le cifrano
- KeePass è un software free che può aiutarti: http://keepass.info/download.html
- KeePass è disponibile anche per Android oltre che per Windows e Linux

Gli strumenti di "Filtro famiglia - Parental Control"

Il filtro famiglia è un software o un servizio in grado di selezionare pagine su Internet in base ad alcuni criteri. Permette di limitare l'esposizione dei bambini a contenuti considerati pericolosi e violenti, soprattutto a questo tipo di pubblico.

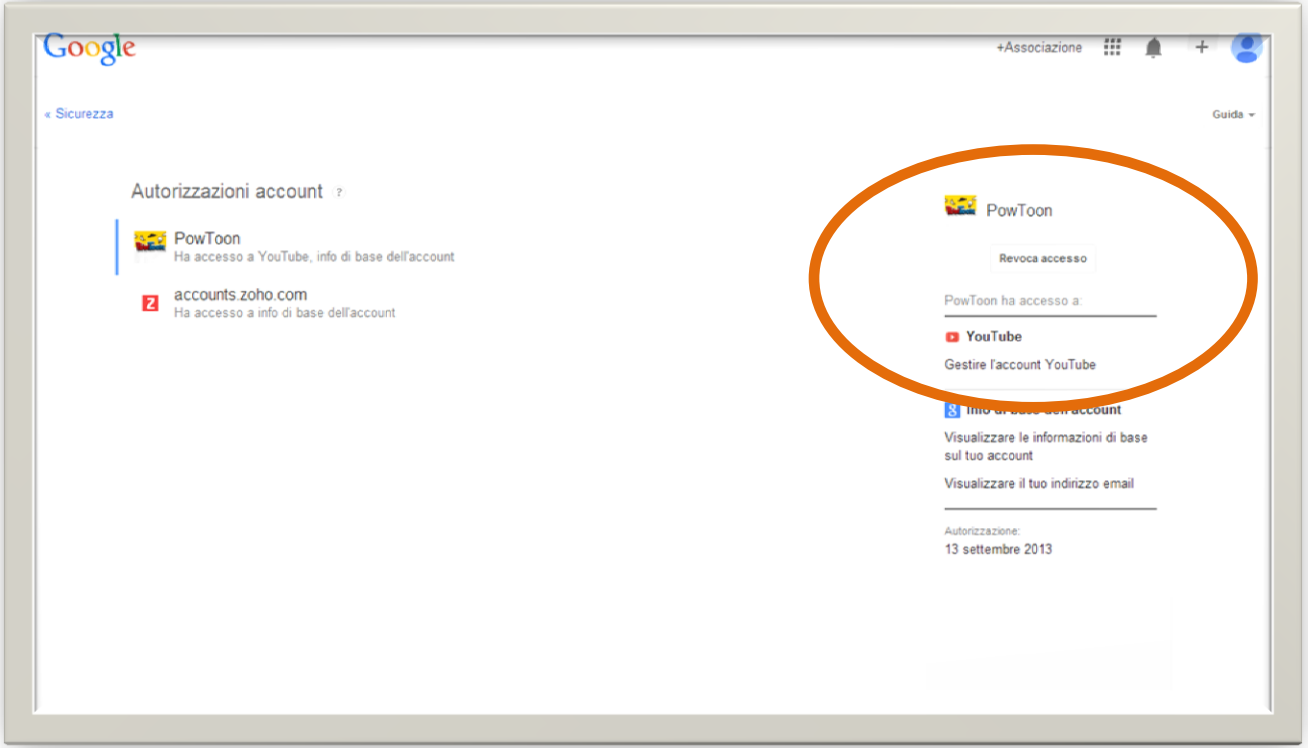
Il filtro famiglia ha generalmente un approccio di blocco di ciò che è considerato non opportuno. Esiste un'alternativa che consiste nell'accettare solo ciò che è positivo. Il filtro quindi non lascia passare nulla che non sia in un elenco di siti approvati dal genitore. È il concetto di "biblioteca di casa" o "walled garden" (giardino recintato).

Esistono in commercio numerosi prodotti di parental control: da software aggiuntivi compresi nelle suite antivirus, fino a complessi apparati hardware da posizionare tra la rete domestica/aziendale e la rete esterna (Internet).

Esiste inoltre il servizio offerto da OpenDNS grazie al quale potrai impostare un Parental Control alla tua connessione Internet per evitare di capitare inavvertitamente su quei siti con contenuti malevoli (pornografici, armi, droga, ecc.), non adatti ad un pubblico di minori. Inoltre potrai maggior tutela anche dai siti di phishing, ovvero quelli che, spacciandosi per portali di banche o enti come le poste, chiedono l'inserimento di dati sensibili come carte di credito o conti correnti per carpirne le preziose informazioni.

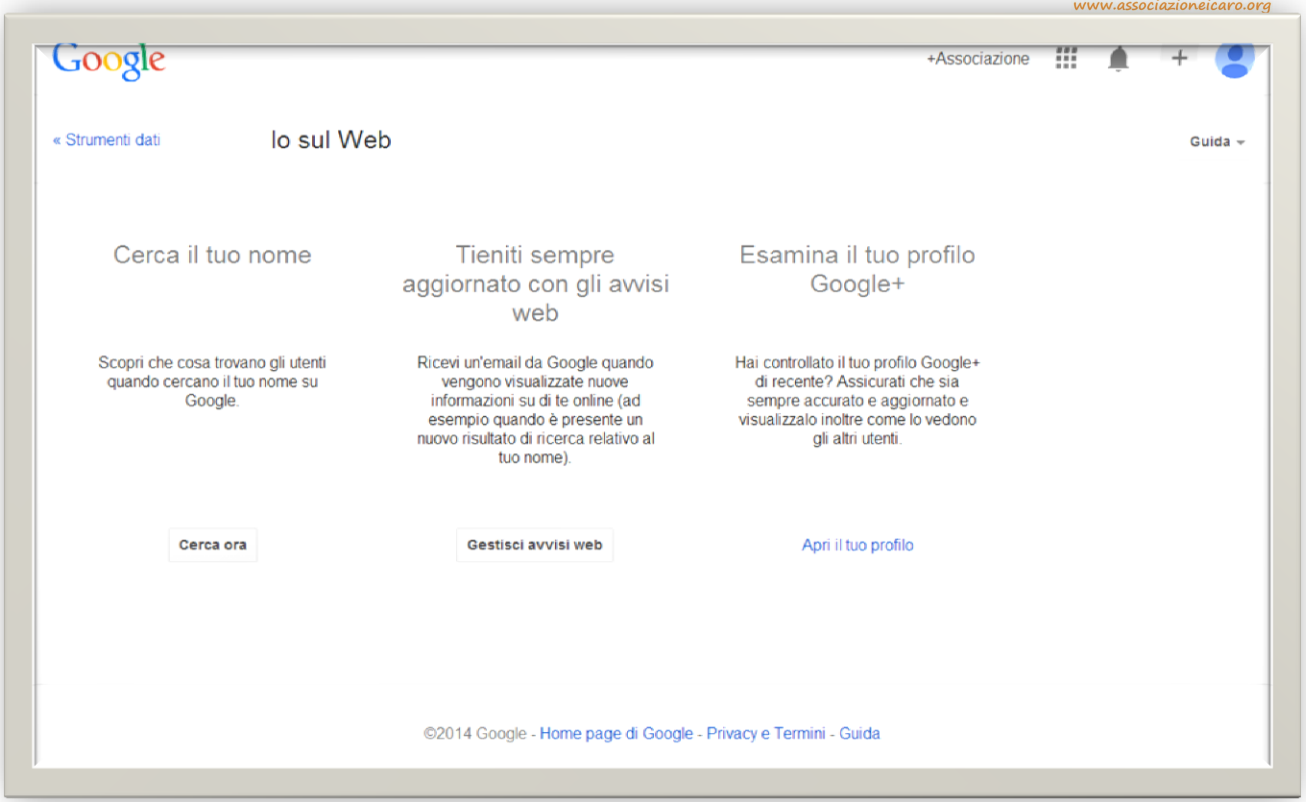
Un'esperienza: privacy e Google in 6 passi

1. Autorizzazioni di accesso all'account
Potrebbe riservare alcune sorprese la voce iniziale del Dashboard "Siti autorizzati ad accedere all'account", in cui possono essere presenti siti per i quali l'utente non ha fornito effettivamente il consenso. In questo caso basta utilizzare il pulsante "revoca l'accesso" per rimuove gli "intrusi".

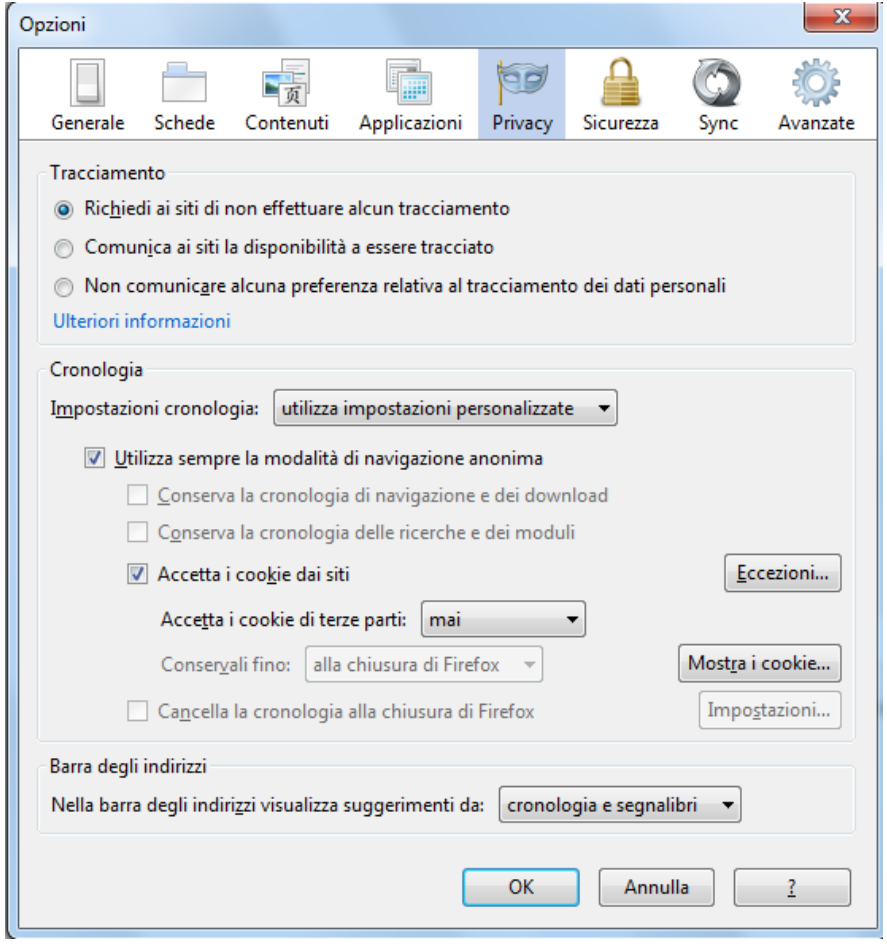


Un'esperienza: privacy e Google in 6 passi

2. “Io sul Web”
Questa sezione dovrebbe servire a gestire l’identità e la reputazione online dell’utente con consigli come “crea un profilo” e “cerca il tuo nome su google”. Il punto in cui si spiega come rimuovere i contenuti indesiderati e i risultati di ricerca associati – procedura sensibile dal punto di vista della privacy, in apparenza chiara e immediata come le precedenti – richiede una lunga serie di passaggi, che vanno eseguiti con pazienza e attenzione.



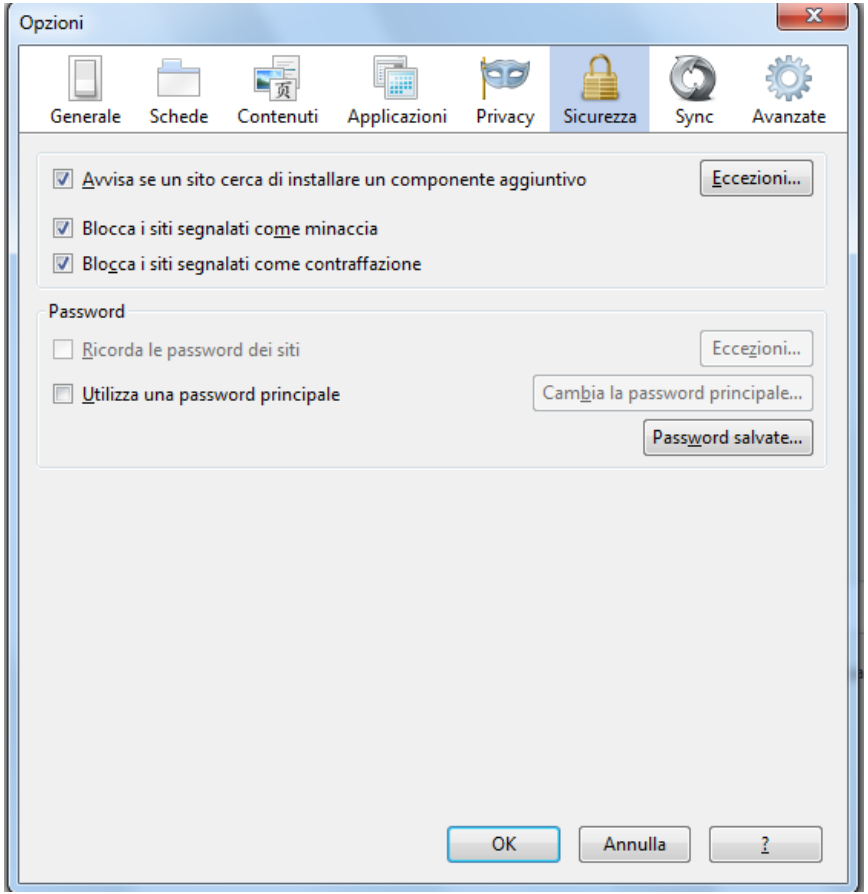
Un'esperienza: privacy e Google in 6 passi



3. La cronologia web

Attraverso la voce cronologia l'utente può gestire l'archivio dei link delle proprie ricerche e impedire a Google di utilizzarle per tracciarne un profilo commerciale. Google facilita questa operazione attraverso l'opzione "cancella cronologia" e il pulsante "sospendi", che dovrebbe impedire la registrazione delle ricerche future. In ogni caso per le proprie ricerche è sempre possibile utilizzare browser diversi da Google Chrome, come ad esempio Firefox, impostando anche in questo caso l'opzione di default "non tracciare". Un altro accorgimento che l'utente può usare è quello di navigare "in incognito", ovvero utilizzare il motore di ricerca Google senza però effettuare il login nel proprio account.

Un'esperienza: privacy e Google in 6 passi

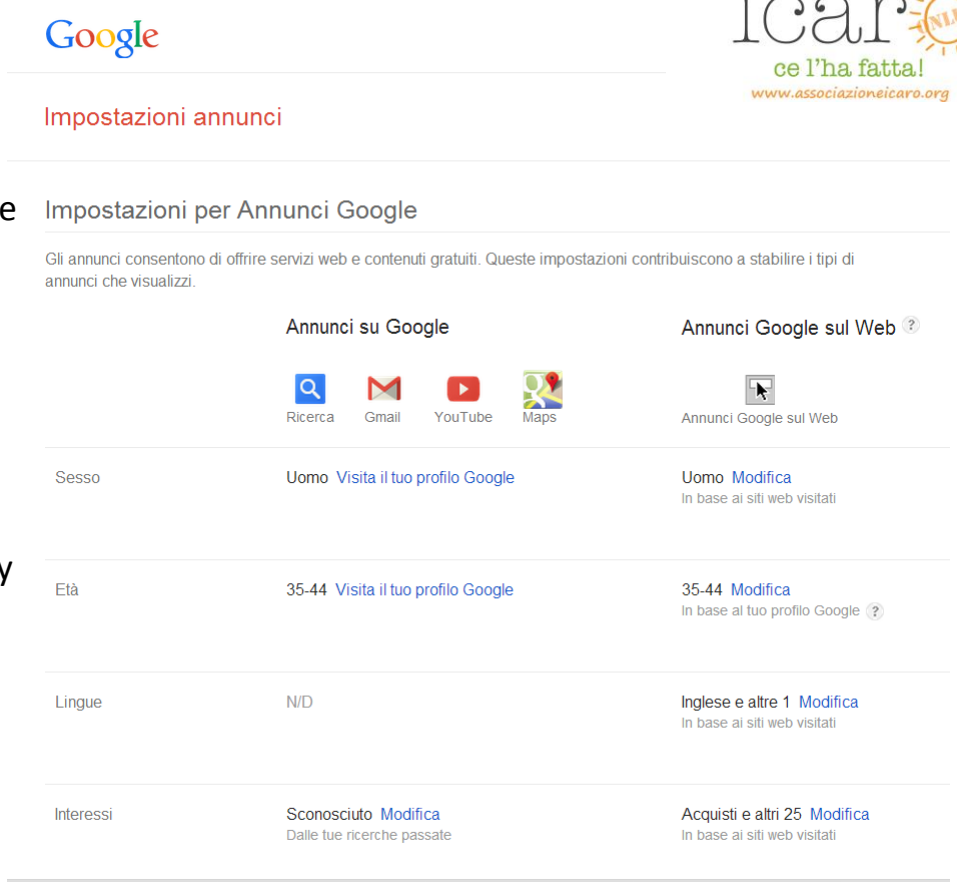


4. La tracciabilità incrociata

Ciò che può lasciare sorpreso l'utente che esplora la sezione cronologia è scoprire che l'elenco dei siti riportati include tutte le ricerche effettuate in qualsiasi momento da qualunque dispositivo, quindi PC, portatili, iPhone, iPad o simili. In questo caso, se l'utente usa il motore di ricerca Google da un iPhone con sistema iOS5, può entrare nelle impostazioni di Safari e attivare l'opzione "Navigazione Privata".

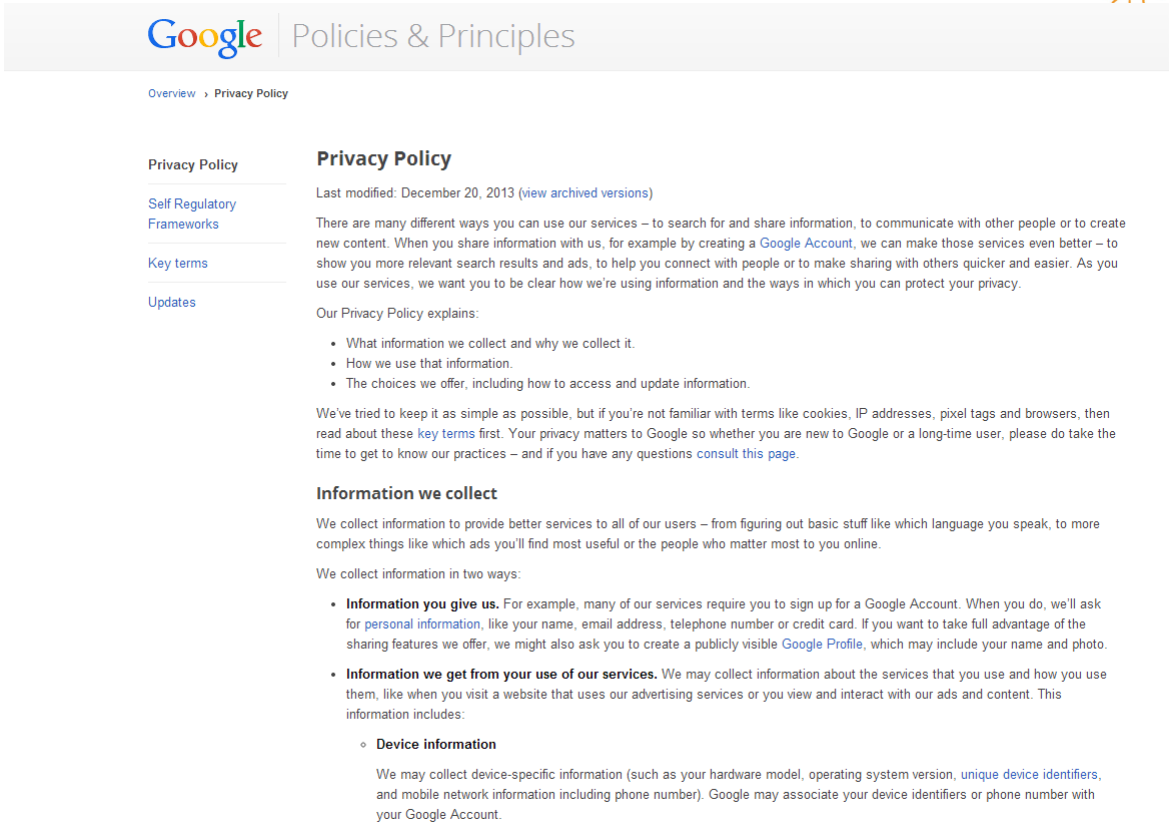
Un'esperienza: privacy e Google in 6 passi

5. Preferenze sugli annunci pubblicitari personalizzati
Sebbene Google consenta di esercitare un controllo sugli annunci personalizzati, i mezzi per farlo non sono immediatamente visibili sul Dashboard. Per effettuare le modifiche l'utente dovrà accedere alla pagina "**preferenze per gli annunci**", e fare clic sul link "**Rimuovi o modifica**" le categorie. L'utente riceve annunci personalizzati se ha consentito a Google di usare i **cookie**, piccoli file scaricati dal browser ogni volta che si effettuano ricerche. Grazie a questi, Big G raccoglie dati e preferenze per proporre annunci pubblicitari ad hoc, dunque per salvaguardare la privacy una scelta conveniente è quella di fare clic su "disattiva"o cancellarli periodicamente. **C'è però una falla nel sistema**: quando l'utente decide di impedire la tracciabilità attiva automaticamente un cookie, che rischia poi di essere rimosso ogni volta che viene eseguita la procedura di cancellazione.



Un'esperienza: privacy e Google in 6 passi

6. “Per motivi legali”
Questa voce prevede che Google fornirà tali informazioni a società, organizzazioni o persone esterne qualora ritenga “in buona fede che l’accesso, l’utilizzo, la tutela o la divulgazione sia ragionevolmente necessario per soddisfare eventuali leggi o norme vigenti, procedimenti legali o richieste governative applicabili”. È chiaro che espressioni come “buona fede” e “ragionevolmente necessario” lasciano uno spazio troppo ampio all’interpretazione, tanto che un coro di obiezioni si è sollevato dai legislatori statunitensi e soprattutto europei, i quali a tutt’oggi considerano questi cambiamenti nella normativa “fuori legge”.


Google Policies & Principles

Overview › Privacy Policy

Privacy Policy

Self Regulatory Frameworks

Key terms

Updates

Privacy Policy

Last modified: December 20, 2013 (view archived versions)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions consult this page.

Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online.

We collect information in two ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.
- **Information we get from your use of our services.** We may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes:
  - **Device information**

    We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

icar ONLUS

ce l'ha fatta!

www.associazioneicaro.org

MY PHONE IS SMART? ME TOO

Sostieni Icaro

con il tuo **5 x mille**

codice fiscale

97592460154

info su

www.associazioneicaro.org