EVITA LE TRAPPOLE ONLINE

Aumenta il tempo che passiamo su Internet e di conseguenza anche il rischio che pirati o truffatori si impadroniscano di informazioni personali o anche dei nostri risparmi

L'epidemia di Coronavirus ha sconvolto le nostre abitudini obbligando la maggior parte delle persone a restare gran parte del tempo in casa, in molti casi anche per lavorare. Il lavoro che viene eseguito da casa si definisce smart o agile e lo si porta avanti usando il nostro computer o al più quello aziendale. Il risultato è quello di aumentare notevolmente le connessioni Internet e il tempo che passiamo in Rete. Lo dimostra un sondaggio appena pubblicato dalla società Context secondo il quale nel mese di marzo il tempo trascorso online è quasi raddoppiato. La stessa AGCOM (Autorità Garanzia Comunicazioni) ha chiesto un aumento del 30% della banda disponibile per evitare possibili blocchi e sia Netflix che Amazon hanno ridotto la qualità del loro streaming per non intasare la Rete. Il vero rischio, però, è che con più gente costantemente collegata aumenti anche il numero dei possibili truffatori che cercano di approfittarne. Attenzione, perché non vi stiamo chiedendo di restare meno tempo su Internet, ma solo di comportarvi in un modo sicuro prendendo le giuste precauzioni. Mai come oggi è indispensabile sapere cosa si può fare e, soprattutto, cosa non è assolutamente il caso di fare quando ci connettiamo online, in modo da proteggere la nostra privacy e quella dei nostri cari.

1 Non fate clic su link che promettono vincite o regali

Per come è costruita la Rete Internet è chiaro che senza fare clic (o tap se usiamo lo smartphone) sui vari link non andremo proprio da nessuna parte. E infatti nei siti "regolari" a ciascun clic corrisponderà solo l'apertura di un'altra pagina o nel caso peggiore quella di una pubblicità particolarmente insistente. Se invece navigando su Internet ci facciamo abbindolare da promesse di premi o di fantomatiche lotterie a cui partecipare con un clic, sarà facile non solo scaricare del malware ma anche ritrovarci con il conto corrente svuotato senza nemmeno rendercene conto.

2 Non scaricate mai contenuti pirata

Cercando su Google si può arrivare a siti pirata in cui sono presenti dei pulsanti, di solito grossi e vistosi, che promettono di farci scaricare contenuti preziosi ma in realtà, nel migliore dei casi, ci collegano a pagine pubblicitarie e in quello peggiore ci fanno installare spyware e barre aggiuntive o sostituiscono in

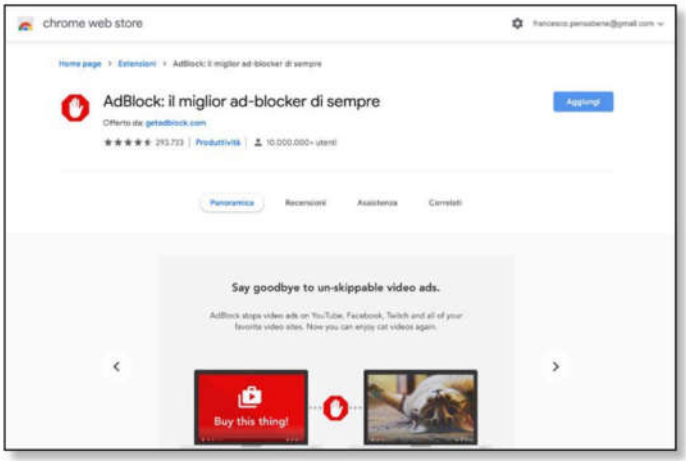
automatico la pagina iniziale del motore di ricerca con una su misura piena di pubblicità. Ma come accorgersi quando un pulsante è fasullo? Prima di tutto evitando siti non conosciuti e che dovrebbero permettere di scaricare gratis contenuti a pagamento. Ma possiamo anche andare con la freccina del mouse sopra il pulsante senza fare clic, nella barra in basso verrà visualizzato l'indirizzo di destinazione. Se non è quello del sito di partenza pensiamoci due volte prima di fare clic.

3 Non aprite i link presenti negli SMS

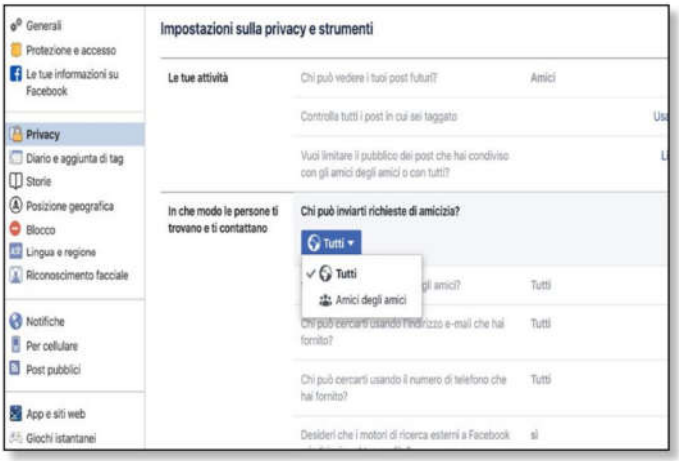
Capita a tutti di ricevere sullo smartphone SMS che ci comunicano che abbiamo vinto un premio o che possiamo partecipare gratuitamente a un concorso con centinaia di premi in palio. E alla fine troviamo un link che di solito è abbreviato e quindi non permette nemmeno di capire dove porta. Non bisogna assolutamente farsi prendere dalla curiosità e farci tap sopra, e questo vale soprattutto se stiamo navigando con la connessione del telefonino. In moltissimi casi, infatti, facendo un tap sul link ci abboneremo a costosi servizi telefonici della cui presenza ci accorgeremo solo controllando la bolletta. Questo vale anche se il mittente è un nome conosciuto come Enel o Telecom. Sono frequenti, infatti, le truffe di questo tipo dove milioni di messaggi vengono inviati ad altrettante utenze telefoniche con la certezza che se anche solo ci cascherà una persona su mille i guadagni saranno ingenti. E purtroppo ad oggi un sistema efficace che rilevi spam per gli SMS non esiste.

COSE DA FARE QUANDO SIAMO ONLINE

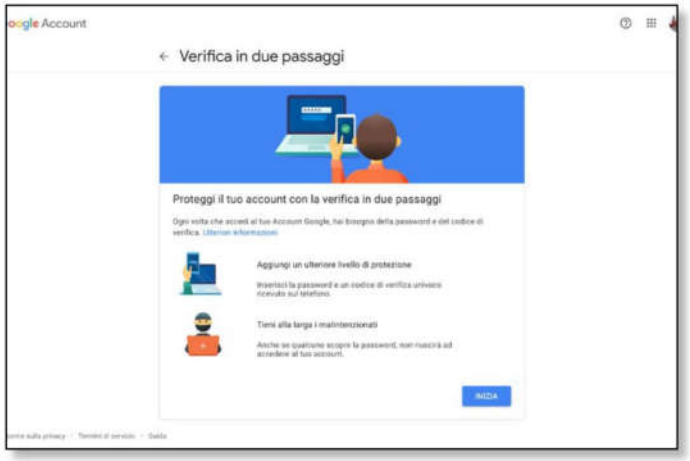
Stare attenti a quali link clicchiamo e ai siti che visitiamo è importante ma non basta. Occorre anche avere strumenti che impediscano di aprire siti pirata e individuino eventuali virus e malware prima che facciano danni. E poi naturalmente è importante avere un doppio sistema di sicurezza non solo per il sito della banca ma anche per i social e per gli account di posta.



1 Installa un adblock Tutti i principali browser come Chrome, Firefox, e Edge permettono di installare delle estensioni e tra queste vi consigliamo proprio AdBlock che eliminerà definitivamente finestre popup e banner dai vostri siti preferiti.



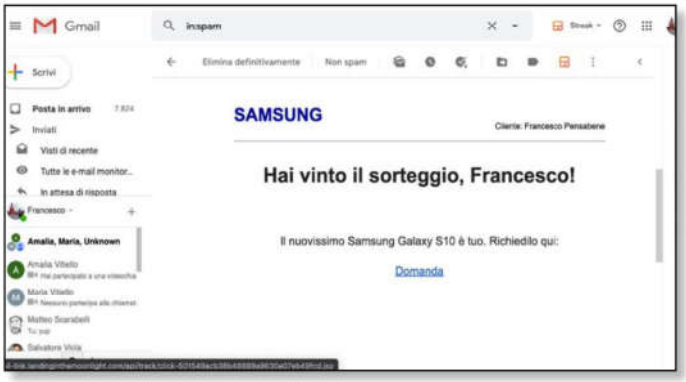
2 Più privacy in Facebook Per eliminare alla radice scocciatori e pirati consigliamo di permettere solo ad amici di amici di chiedere l'amicizia. Possiamo attivare la funzione dalle **Impostazioni** di Facebook nella sezione **Privacy**.



3 Attiva il sistema di verifica a due passaggi. Una sola password, anche se complessa, può non essere sufficiente. Per i siti più importanti, come quello di Google, consigliamo di attivare la doppia verifica da **Impostazioni/Privacy**.

4 Installa un antimalware. Anche se abbiamo già un buon antivirus è consigliabile installare un antimalware per le minacce online. Quello di Malwarebytes offre gratuitamnete il controllo in tempo reale. *https://it.malwarebytes.com*

4 NON DATE RETTA ALLE MAIL DI VINCITE



1 Troppo bello per essere vero. Capita spesso di trovare nella casella di posta fantomatici avvisi di vincite a sorteggi o a lotterie. Se proprio non siamo convinti che si tratti di una bufala, andiamo con la freccina sul link e controlliamo in basso l'indirizzo a cui verremo mandati. Difficilmente sarà quello di chi ha messo in piedi il sorteggio!

2 Sondaggi fasulli. Chi invece decidesse di abboccare si ritroverà al posto della comunicazione di vincita l'invito a partecipare a un fantomatico sondaggio il cui scopo è (nel migliore dei casi) quello di rifilarci pubblicità non richiesta. E nel peggiore quello di installarci sul computer o sullo smartphone un malware o uno spyware.

5 Non fidatevi dei link abbreviati

Il trucco di andare con la freccina del mouse sopra un link per vedere dove porta prima di cliccarci sopra non funziona con i link abbreviati che vengono usati sempre più spesso per rendere più facilmente copiabili link lunghissimi (lo facciamo anche noi con le Super Offerte, per esempio).
Se non siamo certi che il link abbreviato sia sicuro possiamo riallungarlo inserendolo nel sito Web *https://www.expandurl.net/* che, oltre a visualizzare il link originale, fornisce anche informazioni utili per capire se siamo di fronte a un link genuino o a uno fasullo.

6 Non aprite ogni allegato

La maggior parte dei client di posta elettronica riesce ormai a identificare in automatico allegati potenzialmente infetti e ad eliminare il messaggio, ma può sempre capitare che un allegato con malware riesca ad arrivare nella nostra casella di mail. I formati da tenere particolarmente d'occhio, oltre naturalmente agli eseguibili EXE, sono i documenti DOC e PDF e più in generale tutti i documenti di testo che possono contenere un codice eseguibile. In questo caso il suggerimento è quello di non aprire questi file con i classici lettori di PDF come Acrobat Reader o con programmi come Office, ma di visualizzarli prima dal browser in modo da controllarne il contenuto. Questo è possibile se usiamo un servizio di webmail, se invece usiamo un client su PC come Outlook consigliamo di usare l'Anteprima.

7 Attenti a Newsletter non richieste

Se abbiamo la casella di posta intasata da messaggi che ci propongono ogni giorno una ricetta diversa oppure un consiglio per vivere meglio, è normale decidere di volersene sbarazzare una volta per tutte. Sconsigliamo però di seguire il metodo suggerito in fondo alla mail: *Per non ricevere più questa newsletter puoi usare questo link*. Seguendo il link, infatti, dovremo inserire altri dati personali e il rischio è che il numero delle newsletter si moltiplichi. Decisamente meglio contrassegnare il mittente come Spam e lasciare al server di posta la responsabilità di archiviarla nella casella della spazzatura.

8 Non accettate strane richieste di amicizia

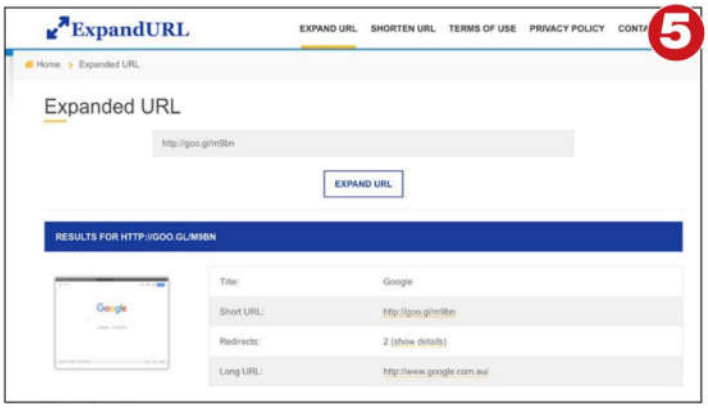
Uno dei sistemi più usati da pirati e truffatori per entrare in contatto con le persone su Facebook è quello di spacciarsi per un vostro conoscente che vi chiede l'amicizia. In molti casi leggiamo il nome di una persona conosciuta e accettiamo la richiesta di contatto senza nemmeno chiederci per quale motivo chi è già nostro amico dovrebbe richiedere un nuovo contatto. Il modo migliore per evitare di trovarsi in questa situazione è quello di oscurare i nomi dei nostri amici dalle impostazioni della **Privacy** di Facebook e allo stesso tempo consentire l'invio di nuove richieste di amicizia solo "Agli amici degli amici". In questo modo la possibilità di ritrovarsi un truffatore tra i contatti di Facebook diminuisce notevolmente.

9 Non pubblicate foto di documenti

Sembra un consiglio scontato, eppure basta dare un'occhiata a social come Instagram o Twitter per trovare ragazzi che hanno appena preso la patente e la mostrano tutti felici ai loro social. Oppure gente che si prende in giro da sola mostrando foto francamente orribili presenti sui documenti. Il rischio, in questo caso, non è tanto quello di rendere pubbliche le nostre fotografie quanto quello di mostrare a chiunque l'indirizzo di casa e soprattutto il numero del documento renden-

10 Non navigate su Internet senza un buon antivirus

Ancora oggi oltre metà delle persone che navigano su Internet non ha installato un antivirus sul proprio computer o smartphone. Se pensiamo che ogni giorno vengono rilevati oltre 200.000 nuovi virus è facile capire come non avere installato un antivirus (o non aggiornare quello che si ha) è decisamente imprudente. Ma quale scegliere? Il miglior antivirus è quello che riesce a garantire un alto tasso di protezione del sistema senza influire troppo sulle prestazioni e con il minimo di "falsi allarmi". Secondo il sito indipendente AV Comparatives, *www.av-comparatives.org*, in questo momento il migliore è Bitdefender, www.bitdefender.it, che è disponibile non solo per Windows ma anche per macOS e Android. Uno dei punti di forza di Bitdefender è il controllo in tempo reale del sistema che è attivo anche nella versione gratuita dell'antivirus.



do così inutilmente semplice la vita ai pirati. Questa raccomandazione vale anche per le targhe delle automobili e delle moto. Ci sono app infatti che permettono di risalire da questi dati a informazioni anche sensibili come assicurazione e bollo auto.

11 Non fate sapere quando non siete in casa

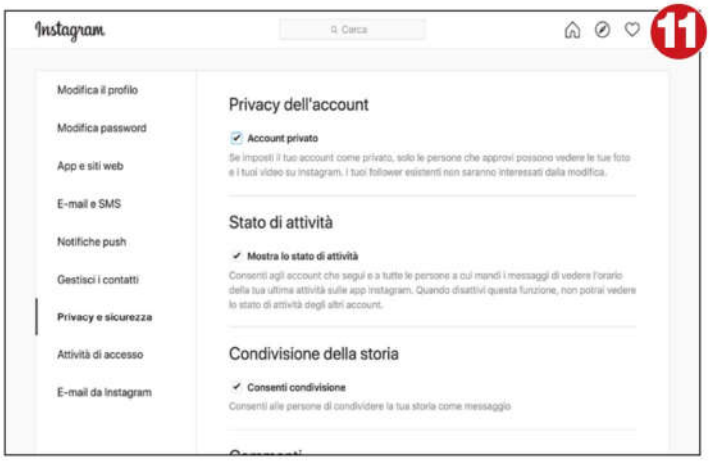
Visto l'obbligo di restare a casa, in questo momento questo non rappresenta un problema, ma ci auguriamo che lo possa diventare la prossima estate. Ci riferiamo alla moda di pubblicare su social aperti a chiunque come Instagram le immagini delle nostre vacanze. Si tratta di un modo sicuro per avvisare ladri e scassinatori che nella nostra casa non c'è nessuno. Se proprio vogliamo pubblicare le foto delle vacanze su Instagram assicuriamoci almeno di rendere privato il social dalle **Impostazioni**, sperando di non avere scassinatori tra i follower. Questo vale anche per Facebook dove è sempre consigliabile limitare al massimo la visibilità.

12 Non usate più volte una sola password

Ci rendiamo conto che non è possibile ricordarsi tutte le password dei servizi a cui siamo registrati, ma allo stesso tempo è importante capire che può essere molto pericoloso usare una stessa password per più account e soprattutto segnarsi le varie password in un qualche documento o nel classico taccuino da portarsi dietro. La soluzione migliore resta quella di utilizzare un servizio come **Last Pass**, *www.lastpass.com* che costruisca per noi ogni volta delle password sicure e soprattutto differenti tra loro. Noi invece dovremo ricordare solo la Master Password ogni volta che vorremo accedere alle Impostazioni. Un secondo suggerimento prezioso è quello di usare quando possibile il doppio sistema di verifica attraverso un SMS sullo smartphone.

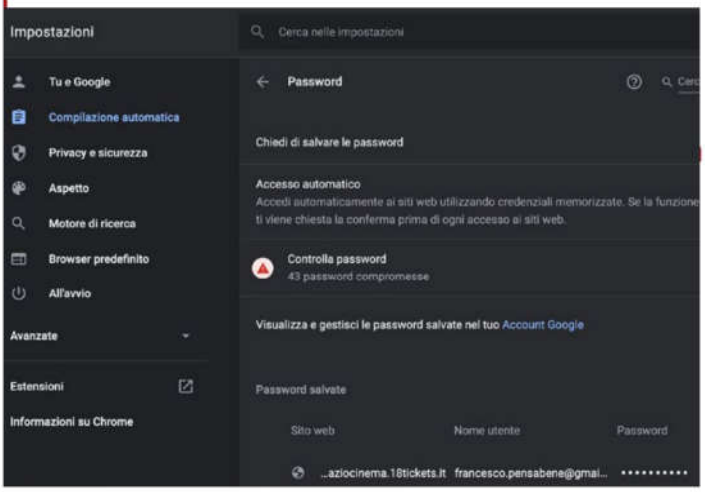
14 Non fidatevi delle reti Wi-Fi gratuite

Soprattutto nelle grandi città oggi è facile trovare reti Wi-Fi



13 Non salvate mai le password nel browser

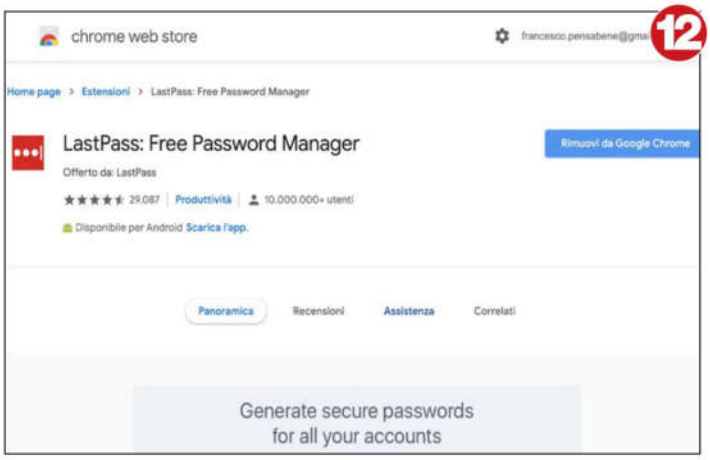
Tutti i browser integrano un sistema che permette di conservare in memoria le password e che può essere impostato in modo da consentire l'accesso automatico a siti protetti come Facebook o anche a siti più "sensibili" come quello della nostra banca. Si tratta di una soluzione apparentemente semplice ed efficace, ma che in realtà mette tutte le nostre password a disposizione di chiunque possa mettere le mani sul nostro computer e rende praticamente inutile tutto il sistema di sicurezza. Con un browser come Chrome, per esempio, basta andare nelle **Impostazioni** e selezionare **Privacy** per visualizzare tutte le password che abbiamo salvato. L'unico sistema di sicurezza previsto dal browser per visualizzare le password è il codice di accesso al computer, che comunque dovrebbe essere conosciuto da chiunque abbia accesso al PC. Per questo motivo è sempre meglio utilizzare un gestore di salvataggio delle password esterno al browser come Last Pass che richiede l'inserimento di una Master Password e volendo anche un sistema di doppia verifica prima di consentire l'accesso ai siti protetti. Un sistema di archiviazione indipendente permette poi di gestire le password da ogni dispositivo, compresi smartphone e tablet. Per questo consigliamo di disattivare la voce **Chiedi di salvare le password** presente nelle **Impostazioni** di Chrome e degli altri browser insieme a quella che consente l'Accesso Automatico al sito.



che offrono l'accesso gratuito all'interno dei centri commerciali, nei ristoranti e naturalmente negli aeroporti e nelle stazioni. Il consiglio è quello di usarle il meno possibile e comunque di non inserire mai dati personali e soprattutto password e dati di carte di credito. Teoricamente, infatti, i nostri dati potrebbero venire spiati, e non stiamo dando la colpa al gestore del negozio o dell'aereoporto, ma a chi imposta il funzionamento della rete Wi-Fi che è spesso facilmente "bucabile". Se proprio non possiamo farne a meno, magari perché siamo all'estero e non abbiamo la possibilità di usare il traffico dati dello smartphone, accertiamoci almeno che gli indirizzi a cui ci colleghiamo siano protetti, che abbiano cioè il suffisso HTTPS con la S finale che indica la presenza di una connessione criptata.

15 Non inserite i dati della carta di credito

Per fare degli acquisti online non è assolutamente necessario inserire ogni volta i dati della nostra carta di credito. Se usiamo abitualmente lo stesso negozio online (per esempio Amazon) basterà inserirli solo la prima volta. Se acquistiamo online da un sito che non abbiamo mai usato, è consigliabile invece utilizzare servizi come quello offerto da PayPal, **www.paypal.com** che non solo richiede di salvare una volta per tutte i dati della carta, ma offre anche un'assicurazione nel caso non dovesse arrivarci il prodotto acquistato. Oltretutto molte banche oggi per fare acquisti con la carta di credito richiedono un doppio sistema di controllo che obbliga ad avere sottomano uno smartphone e



12

che risulta spesso poco pratico. In alternativa è sempre possibile usare una carta prepagata, per esempio la Postepay, che contiene una quantità di denaro che può essere limitata al prezzo di quello che vogliamo acquistare. In questo modo anche se i pirati dovessero clonarcela, i danni sarebbero limitati.

16 Non condividete foto hot

Purtroppo una volta che un'immagine viene pubblicata online poi diventa praticamente impossibile eliminarla. E questo può valere anche per le condivisioni tra fidanzati o amici di immagini hot. Per evitare di pentirsi in un secondo momento è meglio evitare di condividere immagini che non vorremmo fossero viste da chiunque. E questo vale anche con un social come **Snapchat** dove le immagini si possono autoeliminare dopo pochi secondi. Tutto quello che arriva online può essere sempre copiato da qualcun altro e venire usato contro di noi.

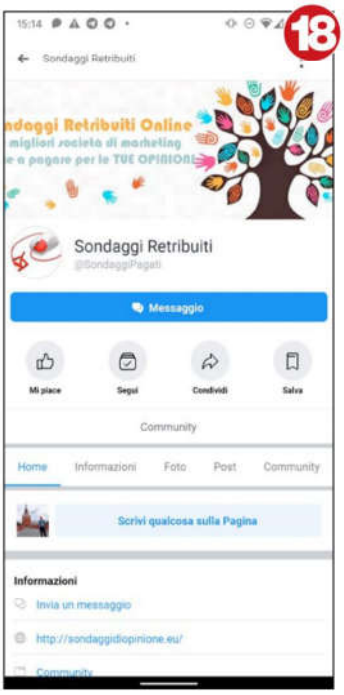
17 Non fate clic sui pop-up

Nella maggior parte dei casi le pubblicità pop-up, cioè quelle finestre o riquadri che compaiono automaticamente mentre navighiamo, sono solo una grossa scocciatura. Evitate però di cliccarci sopra, anche se promettono fantastici premi. Chi usa Chrome potrà risolvere il problema alla radice disattivandoli dalle **Impostazioni Avanzate** selezionando **Privacy e Sicurezza** e quindi **Impostazioni Sito** e **Autorizzazioni/Popup**.

18 Evitate quiz e sondaggi

Soprattutto su Facebook siamo circondati da proposte di giochi, quiz, ricerche di mercato e sondaggi che molto spesso portano a siti esterni che nel migliore dei casi visualizzano pagine su pagine di pubblicità non richiesta. Oltretutto, soprattutto con i sondaggi e le ricerche di mercato, ci verranno sempre richiesti i nostri dati personali, a partire dalla mail, e molto spesso finiremo all'interno di catene di pubblicità non voluta.

Quando andrete finalmente in vacanza non condividete la notizia in tempo reale. Potreste ricevere visite non gradite a casa!



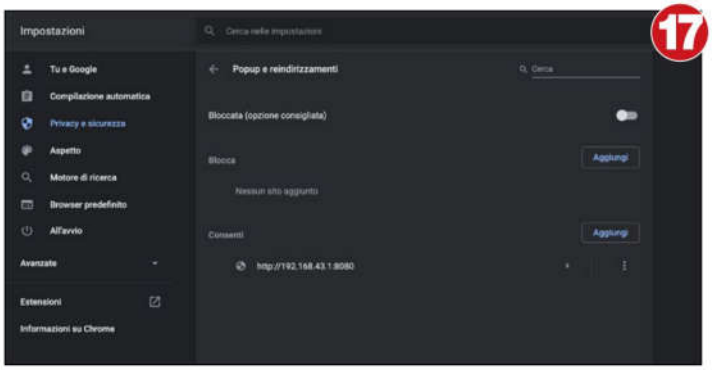
18

19 Non fatevi l'autodiagnosi online

Siamo tutti un po' ipocondriaci e per ogni disturbo che sentiamo di avere è sempre possibile trovare online informazioni terrorizzanti o peggio ancora consigli per cure fai-da-te. Il risultato di una ricerca di questo tipo può diventare alla lunga dannoso per la nostra salute e nel migliore dei casi creare tanto stress inutile. Solo se dopo un reale controllo medico scopriremo di avere un problema serio potremo iscriverci a uno dei tanti gruppi di auto-aiuto disponibili online.

20 Non collegate social tra loro

Condividere contenuti e immagini va bene, a condizione però di non esagerare. Postare su più social contemporaneamente per esempio può non essere sempre una buona idea. Le regole di accesso ai vari social sono infatti diverse e mentre solamente i nostri amici possono vedere le immagini che pubblichiamo su Facebook, nella maggior parte dei casi non è così per Twitter o Instagram. E ritrovarsi le foto di una festicciola o di un aperitivo disponibili per chiunque non è sempre piacevole. A meno di non decidere di rendere privato l'accesso anche agli altri social che abbiamo!



17

I truffatori del Coronavirus

Come se non bastasse l'obbligo di restare chiusi in casa e la paura di beccarsi il virus anche solo andando a fare la spesa, ci si mettono anche i soliti truffatori che cercano di approfittarsi della paura collettiva per guadagnare qualche euro. Attenzione perciò ai video condivisi (magari in buona fede) da qualcuno su WhatsApp o agli SMS in cui si chiedono offerte per ospedali o fantomatiche associazioni benefiche. Non stiamo invitandovi a non donare, ma solo a farlo con attenzione. La RAI e molti quotidiani come il Corriere della Sera hanno organizzato donazioni per i singoli ospedali, così come hanno fatto Fedez e Chiara Ferragni. Ma sono tutte organizzazioni e persone facilmente riconoscibili e che comunque è possibile contattare telefonicamente o attraverso un sito Web. Poi certo, anche i singoli ospedali accettano donazioni, ma prima di farle vi consigliamo di accertarvi a chi state inviando i vostri soldi!