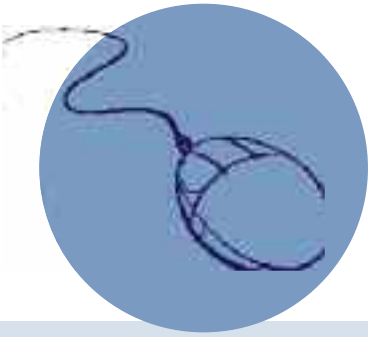


La Borsa *della* Spesa
Edizione 1.15

Doppioclick:
Bloccare le Smart TV troppo pettegole

Se avete una cosiddetta "Smart TV", di quelle che si possono comandare con i gesti e con la voce, tenete presente che questi dispositivi possono ascoltarvi costantemente e trasmettere a terzi tutto quello che dite nelle loro vicinanze quando sono in funzione o in standby.

Questa caratteristica sorprendente è poco pubblicizzata, ma è documentata per esempio sul sito della Samsung come segue: "Siete pregati di tenere presente che se le vostre parole pronunciate includono informazioni personali o altre informazioni sensibili, tali informazioni faranno parte dei dati catturati e trasmessi a terzi tramite il vostro uso del Riconoscimento Vocale".

Il riconoscimento delle vostre parole, infatti, non viene effettuato direttamente dal televisore: i suoni captati dal suo microfono vengono trasmessi via Internet a un servizio esterno, che analizza la vostra voce e restituisce al televisore i comandi vocali riconosciuti. Se la trasmissione viene intercettata, per esempio perché la Smart TV è connessa tramite una rete Wi-Fi poco protetta, il televisore diventa una costosa "cimice" involontaria.

Quest'analisi è, tuttavia, disattivata in fabbrica e si attiva soltanto se l'utente accetta clausole apposite, tramite vari clic espliciti, durante l'impostazione iniziale della Smart TV; inoltre non può funzionare se il televisore non è connesso a Internet. Se non ricordate se avete accettato o meno il riconoscimento vocale, andate nelle impostazioni del dispositivo e controllate queste clausole, disattivandole se necessario. In alternativa, in alcuni modelli di Smart TV è possibile usare un apposito tasto del telecomando come interruttore per aprire e chiudere il microfono, evitando che sia perennemente in ascolto.

Le Smart TV sono solitamente dotate anche di una piccola telecamera che serve per riconoscere i gesti e i volti ed è costantemente attiva: se questo causa disagio oppure è proibito o inopportuno, come negli spogliatoi o nei camerini, il rimedio più efficace è scollegare la telecamera oppure ruotarla o coprirla in modo che non possa vedere nulla.

Paolo Attivissimo

La Borsa *della* Spesa
Edizione 2.15

Doppioclick:
Stufi di aggiornare Flash insicuro? Toglietelo

Flash di Adobe è un software diffusissimo sui personal computer di tutti i tipi: serve principalmente per mostrare video, animazioni e pubblicità nelle pagine del Web. Se visitate www.adobe.com/software/flash/about e compare una F stilizzata e animata, avete Flash. Purtroppo questo software ha un grosso difetto: è molto vulnerabile. Soltanto nel 2015 sono state rivelate in Flash oltre 30 falle distinte, al punto che è oggi il bersaglio preferito degli attacchi informatici. Spesso basta visitare una pagina di Internet per infettare un computer dotato di Flash. Inoltre c'è la scocciatura di dover installare i suoi continui aggiornamenti: ben sedici negli ultimi otto mesi.

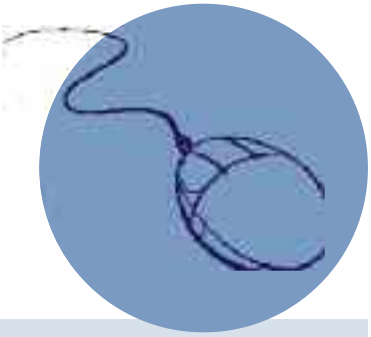
Dato che i siti che richiedono Flash sono in rapido calo (anche Youtube non lo richiede più), molti esperti consigliano di disinstallarlo per evitare i fastidi di aggiornamento e soprattutto le sue falle di sicurezza. Le istruzioni sono presso Adobe.com.

Se non volete rinunciare del tutto a Flash ma volete comunque ridurne i rischi, potete impostare il vostro browser (l'app che usate per sfogliare le pagine del Web) in modo che vi chieda il consenso prima di attivare Flash: questo evita che un sito ostile possa usare questo software per attaccarvi e ha il beneficio aggiuntivo di bloccare molte pubblicità animate fastidiose.

Per Firefox, andate in Strumenti - Componenti aggiuntivi - Plugin e impostate Shockwave Flash a "Chiedi prima di attivare". Per Chrome, scegliete Impostazioni - Mostra impostazioni avanzate - Privacy - Impostazioni contenuti - Plugin - Blocca per impostazione predefinita. Per Safari, scegliete Preferenze - Sicurezza - Plugin Internet: cliccate su Impostazioni siti web, selezionate Adobe Flash Player e impostate a "Chiedi" tutti i siti eventualmente elencati; ripetete per il menu a discesa Quando visito altri siti web. Per Internet Explorer, andate in Impostazioni (icona dell'ingranaggio in alto a destra) - Gestione componenti aggiuntivi - Mostra: tutti i componenti aggiuntivi - Shockwave e scegliete Disabilita.

Un altro trucco molto pratico è disinstallare Flash ma installare Google Chrome: questo browser, infatti, include una propria versione di Flash meno insicura di quelle normali. Si naviga normalmente con Firefox, Safari o Internet Explorer, e quando si incontra un sito che richiede Flash lo si apre con Chrome.

Paolo Attivissimo



La Borsa *della* Spesa
Edizione 3.15

Doppioclick:
I nostri "selfie" sfruttati per vendere

Se pubblicate su Instagram, Twitter o Tumblr una vostra foto che include un marchio famoso (per esempio sulla bibita che avete in mano o sugli abiti che indossate), tenete presente che potrà essere analizzata e sfruttata a fini di marketing dai vari sistemi automatici che riconoscono questi marchi e vendono le proprie analisi alle aziende. Il vostro "selfie" mentre bevete una birra o indossate una felpa con un logo sportivo, insomma, può essere preso e usato a vostra insaputa per trarne guadagno.

È legale? Sembra proprio di sì, perché i servizi di analisi di massa delle foto usano soltanto le immagini che voi permettete a chiunque di vedere, mentre le foto "private" o riservate agli amici non vengono esaminate: abbiamo insomma dato il nostro consenso implicito quando abbiamo pubblicato le foto. Ma è un uso probabilmente inaspettato delle nostre immagini personali. Un uso che vale oro, considerato che le foto non solo mostrano il sesso e l'età della persona che usa il prodotto ma illustrano anche il contesto d'uso e soprattutto sono accompagnate da dati sul luogo e l'ora di scatto e quindi permettono di sapere con precisione come, dove, quando e in quali gruppi di consumatori circola un marchio, ottenendo quindi ricerche di mercato capillari, in tempo reale e a costi bassissimi.

Per vedere all'opera questi sistemi di riconoscimento automatico, visitate per esempio Streamditto.com, sito promozionale della Ditto Labs: vi troverete un flusso costante di immagini di internauti, tratte dai principali social network (Facebook per ora è escluso), nelle quali viene evidenziato il marchio riconosciuto. Potete scegliere fra varie categorie (birre, abbigliamento, auto, sport e altro ancora) e apprezzare quant'è sorprendentemente abile il riconoscimento anche quando il logo è parzialmente coperto oppure distorto.

Si può sfuggire a questo sfruttamento commerciale delle nostre immagini? In parte sì, per esempio evitando di mettere sui social network foto visibili a tutti e disattivando la localizzazione sul telefonino usato per scattare le immagini: fra l'altro, questo è utile anche per non esporsi a bulli digitali e stalker. Ma i social network vivono di dati personali, per cui se scegliamo di frequentarli troveranno sempre il modo di sfruttarli e sfruttarci.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 4.15

Doppioclick:
Telefonini vecchi.Non buttateli, convertiteli!

La corsa veloce della tecnologia e del consumismo ci porta spesso ad avere nel cassetto telefonini che non usiamo più anche se sono perfettamente funzionanti. Ma ci sono molti modi per ridare nuova vita a uno smartphone senza per forza rottamarlo.

Per esempio, se avete un telefonino che è diventato impresentabile a causa di graffi o cadute, potete trasformarlo in un hotspot Wi-Fi, utile specialmente all'estero se vi inserite una SIM per trasmissione dati del paese che state visitando: lo terrete in borsa o in tasca e avrete sempre con voi la rete Wi-Fi personale per tutti i vostri dispositivi.

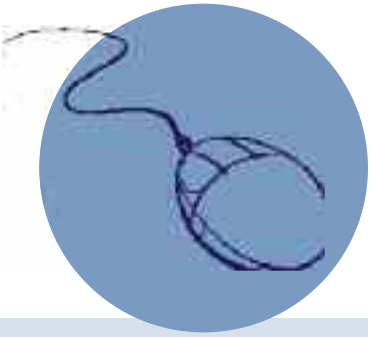
Non trovate un lettore audio portatile capace di contenere tutta la vostra musica? Togliete foto, giochi e video da un vostro vecchio smartphone e avrete spazio in abbondanza per la vostra collezione di brani, specialmente nei modelli che hanno schede di memoria rimovibili. E se la vostra auto ha un ingresso audio o un ricevitore Bluetooth, mettete lo smartphone riciclato in modalità aereo (per ridurre le emissioni e far durare la batteria) e installate per esempio Car Music Player, un'app che offre comandi grandi e intuitivi e tiene sempre acceso lo schermo, per avere un'autoradio-jukebox a costo zero.

Uno smartphone può anche diventare un telecomando per computer e media center, se gli installate Gmote, VLC Remote Free o Remote e lo collegate alla vostra rete Wi-Fi.

Si può inoltre convertire un cellulare in una memoria mobile con Wi-Fi integrato per condividere i file: basta inserire nel telefonino una scheda di memoria capiente e sarà possibile trasferire foto via Wi-Fi o Bluetooth oppure con un semplice cavo USB. Queste funzioni sono già incluse nello smartphone e non occorre installare nulla.

Vi serve una telecamerina di sorveglianza? Collegate il vecchio smartphone alla rete Wi-Fi e installate Qik o IP Webcam per trasmettere in streaming dal vostro telefonino. Infine, invece di acquistare una dashcam (telecamera che videoregistra e documenta automaticamente gli spostamenti in auto), convertite uno smartphone usando un supporto per auto e un'app come CamOnRoad oppure AutoGuard. Molte di queste app richiedono una SIM nel telefonino, ma non occorre attivare un contratto: si può usare tranquillamente una vecchia SIM disattivata.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 5.15

Doppioclick:
Limitare il tempo d'uso di tablet e telefonini

Il tempo vola quando si gioca, si chatta o si sfoglia il Web su un telefonino o su un tablet; spesso staccarsi è difficile, e staccare i figli da questi schermi così accattivanti a volte pare impossibile. Sorvegliarli con il cronometro in mano è impraticabile, per cui un aiutante informatico può essere utile.

Per l'iPad e l'iPhone c'è un sistema incorporato molto semplice: per prima cosa si imposta un codice di blocco, andando in Impostazioni – Codice – Abilita codice, digitando il codice scelto e avendo cura di disattivare Inizializza dati. Poi si lancia l'app Orologio, si sceglie Timer, si imposta il limite di tempo che si desidera e come suoneria si sceglie Interrompi Riproduzione. Toccando Avvia inizia il conto alla rovescia del tempo assegnato all'uso del dispositivo. Quando scade il tempo, il tablet o telefonino si blocca inesorabilmente.

Per i telefonini e tablet Android (praticamente tutte le marche diverse da Apple) bisogna installare delle app specifiche, come per esempio Kids Place della Kiddoware (gratuito in Google Play), che oltre a impostare un limite di tempo generale blocca lo scaricamento e l'acquisto di altre app e inibisce le chiamate in arrivo. Se si preferisce un limite di tempo specifico per i video di Youtube, c'è Youtube Kids di Google, gratuito in Google Play, che inoltre filtra i video non adatti ai bambini.

Per limitare non solo il tempo ma anche le fasce orarie, sui dispositivi Android si può usare Screentime (40 dollari/anno presso Screentimelabs.com), che permette anche il controllo e la gestione a distanza e consente di selezionare una per una quali app possono essere usate.

Gli ausili tecnici ci sono, insomma, ma è consigliabile affiancarli al dialogo e a un'offerta di altre attività interessanti e magari più educative e sociali.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 6.15

Doppioclick:
Ricattati da una videochat intima, che fare?

Lui e lei s'incontrano in uno dei tanti servizi di chat video di Internet; lei si dimostra subito molto disinibita e si offre man mano allo sguardo di lui e lo invita a fare altrettanto. Lui ci sta e si esibisce, i due si scambiano i contatti su Facebook, ma di colpo la trasmissione video s'interrompe e lei gli rivela che lui è stato videoregistrato e che la registrazione verrà pubblicata su Youtube, Dailymotion o altri siti simili e inviata ai suoi amici (scoperti tramite Facebook) se non paga qualche migliaio di franchi. Panico.

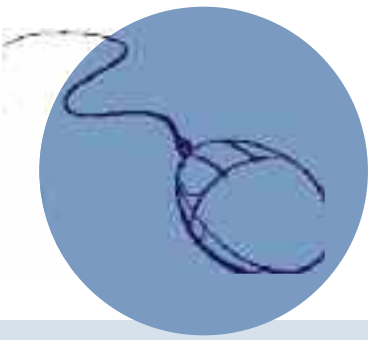
Ho seguito numerosi casi come questo: la prima cosa da fare è non pagare, perché se ci si dimostra ricattabili si riceveranno soltanto ulteriori richieste di denaro. Bisogna ricordarsi, inoltre, che non si è commesso alcun reato se l'interlocutore della chat era chiaramente maggiorenne. I truffatori a volte dicono che la chat intima è stata vista da una bambina, ma è una bugia per mettere paura.

In realtà i truffatori lavorano sui grandi numeri, per cui se si oppone resistenza spesso lasciano perdere per passare alla vittima successiva. Per esempio, si può bluffare dicendo che la pubblicazione non causerà imbarazzo ma solo qualche risata degli amici, e che la vicenda è già stata segnalata, o lo sarà a breve, ai siti coinvolti e alla polizia. Inoltre chi è minorenne può dire di non avere soldi per pagare. Queste risposte in molti casi fanno desistere di colpo i criminali.

Inoltre conviene controllare se l'account della ragazzaesca e quello dove i truffatori minacciano di pubblicare il video esistono ancora: se non ci sono più, vuol dire che sono già stati segnalati come criminali da vittime precedenti e quindi chiusi dai servizi di sicurezza dei rispettivi siti. Se esistono ancora, la vittima li può segnalare: verranno chiusi prontamente.

I truffatori dovranno perdere tempo a creare account nuovi e avranno difficoltà a ricontattare le proprie vittime, per cui tipicamente lasceranno perdere i già truffati e cercheranno nuovi bersagli. E una volta scampato il pericolo, un adesivo che copra la telecamera del computer sarà un buon promemoria di essere meno imprudenti in futuro.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 7.15

Doppioclick:
Pubblicità che infetta, come difendersi

Il crimine informatico non dorme mai e inventa continuamente nuovi metodi per guadagnare alle spalle degli utenti. L'ultima novità è il malvertising: pubblicità infettanti visualizzate all'interno di siti rispettabili.

Chi le clicca si trova con tutti i dati del computer lucchettati da una password che conosce soltanto il criminale, che la fornisce alla vittima dietro pagamento di un riscatto. Chi non paga e non ha una copia di scorta dei propri dati perde tutto. L'attacco è particolarmente efficace perché avviene all'interno di siti normalmente considerati sicuri, come per esempio quello del popolare quotidiano britannico Daily Mail o del sito d'incontri Match.com.

I siti che ospitano questi attacchi sono innocenti: si limitano a ospitare pubblicità raccolte da agenzie pubblicitarie esterne. I criminali si spacciano per inserzionisti e forniscono gli spot; le agenzie non si accorgono che gli spot sono infetti, e la trappola scatta.

Difendersi richiede un buon antivirus (che già dovrebbe esserci) e l'aggiunta di filtri blocca-pubblicità, come Adblock (https://adblockplus.org) o uBlock www.ublock.org), entrambi gratuiti e disponibili per quasi tutti i principali programmi di navigazione (Chrome, Firefox, Opera, Safari). Conviene inoltre impostare Adobe Flash in modo che chieda il permesso prima di avviare qualunque video o animazione (come descritto presso http://tinyurl.com/blocca-flash), visto che questi attacchi spesso usano Flash.

Bloccare le pubblicità esterne non solo aumenta la sicurezza ma velocizza la navigazione: per contro riduce gli introiti dei siti visitati. Conviene quindi farlo con giudizio caso per caso, per non penalizzare i siti che dipendono dagli spot, in attesa che adottino soluzioni pubblicitarie meno vulnerabili e meno pericolose per noi utenti. E magari, già che ci siamo, un po' meno invadenti.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 8.15

Doppioclick:
App che ci spiano, anche a fin di bene

Le app da installare di nascosto sui telefonini altrui per spiare movimenti, messaggi e chiamate non sono un mito: esistono davvero, specialmente per i telefonini Android, sui quali sono più facili da installare rispetto agli iPhone. Si comprano fuori dai negozi ufficiali come App Store o Google Play, perché la loro legalità è incerta; le usano soprattutto i genitori ansiosi, gli investigatori e i partner gelosi.

Il modo più semplice per difendersi da queste app "spione" è usare un telefonino semplice, non "smart"; se questo non è possibile, lo smartphone va protetto con un PIN lungo o con l'impronta digitale e non va mai lasciato incustodito.

Se è un Android, va inoltre dotato di antivirus; se è un iPhone, non va "craccato" togliendogli le protezioni standard, come fanno invece molti utenti. E naturalmente si può sempre lasciare a casa il telefonino, e usare un altro telefono per fare chiamate, quando non si vuole essere pedinati digitalmente.

Ci sono però anche app di sorveglianza "oneste" che non si nascondono: le installano per esempio le famiglie, così i genitori sono più tranquilli perché sanno automaticamente quando arrivano a scuola o rincasano i figli (che non devono più ricordarsi di fare squilli), oppure i gruppi in gita, per rintracciare i dispersi. Una delle app più popolari di questo tipo è Life360, disponibile per iPhone, Android e Windows Phone (www.life360.com) e gratuita nella versione di base: usa la geolocalizzazione offerta da tutti gli smartphone per mostrare sui rispettivi schermi una mappa, aggiornata in tempo reale, di dove si trova ciascun membro della famiglia o del gruppo.

L'aggiornamento viene trasmesso da ciascun utente via Wi-Fi oppure sulla rete dati cellulare e sono disponibili una cronologia delle posizioni passate e la notifica via mail quando viene raggiunto o lasciato un luogo predefinito (casa, scuola, lavoro).

I dati di posizione sono visibili soltanto ai membri di una famiglia o di un gruppo, che possono inoltre scambiarsi messaggi privati senza i costi degli SMS tradizionali, e ogni membro è libero di appartenere a uno o più gruppi (o "cerchie", nel gergo di Life360) e di scegliere in ogni momento a chi far sapere o non sapere la propria posizione. C'è anche una funzione di allarme per le emergenze. È insomma una sorveglianza su base volontaria e consensuale, che si rivela utile e poco invadente.

PAOLO ATTIVISSIMO