ANNO 2 NUMERO 1

FunMagazine

Giugno 2017

In questo numero

TUTTO CIÒ CHE GOOGLE CONOSCE DELLE ABITUDINI DIGITALI DI OGNUNO

Non è soltanto una leggenda metropolitana quella che vuole che Google sia a conoscenza di tutte le abitudini digitali degli internauti.
Non è necessario essere un utilizzatore di cellulari con sistema operativo Android, o navigatori che prediligono il browser Google perché Google registri tutte le attività che si compiono sulla rete Internet.

E' sufficiente collegarsi ad un motore di ricerca, ad un social network, come pure ad un qualsiasi sito internet, perché vengano raccolti dei dati e delle informazioni sui comportamenti e le preferenze di navigazione, che riguardano l'utente che vi accede.

L'incrocio di tutte le informazioni rilevate, rendono possibile a Google, con delle opportune analisi dei dati registrati, arrivare a conoscere con una buona approssimazione l'orientamento politico, religioso e sessuale di chiunque.

Ma ognuno può divenire maggiormente consapevole di ciò che Google conosce dei propri comportamenti digitali accedendo all'indirizzo https://history.google.com/history/

Nel riquadro statistiche è possibile visualizzare dei periodi temporali di osservazione delle ricerche effettuate sul motore, o su YouTube, o sulle applicazioni Android.

"Google può ricavare orientamento politico religioso e sessuale di chiunque"

Cliccando poi sull'icona con i tre puntini in verticale, accederete a un menu aggiuntivo da cui è possibile anzitutto cancellare i dati sulle attività Web secondo diversi criteri, scaricare le ricerche effettuate e cambiare le impostazioni riguardo ai dati che devono o meno essere raccolti, cliccando su Impostazioni/Mostra altri comandi.

Inoltre, scorrendo la pagina fino alla voce Impostazioni correlate e cliccando su Annunci, si potrà accedere a una pagina che contiene il profilo ricavato dall'analisi dei dati e delle preferenze.

Troverete infatti qui sesso ed età ipotizzati e un elenco dei principali temi di interesse, oltre ad altre opzioni per aiutarvi a focalizzare ancora di più le

E' SICILIANO IL SOFTWARE PER SCRIVERE IN INGLESE

Un team di ragazzi programmatori siciliani ha creato un software per scrivere in perfetto inglese. Il traduttore di Google è certamente una soluzione sbrigativa per tanti, ma non riesce ad essere privo di errori di interpretazione dei testi e quindi non risulta essere sicuro al cento per cento.

Tutti i programmatori del team hanno meno di 35 anni ed hanno sviluppato il software di traduzione italiano – inglese, che hanno battezzato "Ludwig", nome del filosofo Wittgenstein, che aveva espresso in una sua frase quella che era la sintesi del progetto ambizioso dei ragazzi: "i limiti del mio linguaggio sono i limiti del mio mondo abbattere la torre di Babele per metterci tutti sullo stesso piano".

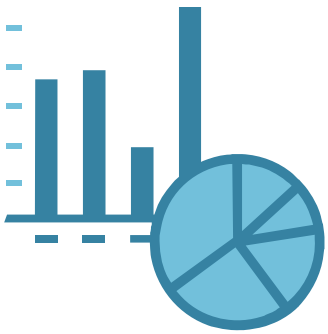
Un software per scrivere in inglese

E' così divenuto il primo motore di ricerca linguistico che aiuta chi deve scrivere in inglese, fornendo traduzioni contestualizzate. Ludwig è in tutto e per tutto un dizionario interattivo, basta scrivere una frase e questa viene tradotta.

L'ideatore del software è Antonio Rotolo, di 35 anni che ha rilasciato all'Huffington Post la seguente dichiarazione: "Sono un ricercatore internazionale e da 25 anni scrivo e parlo in inglese. La conoscenza di un non-nativo, tuttavia, non è mai sufficiente. Questo produce un gap di capacità e competenze, compromettendo la possibilità di competere sul mercato. L'inglese ormai è la lingua del mondo, per ciò ho pensato fosse fondamentale che a tutti venisse data la possibilità di comunicare sullo stesso livello"

Il progetto è stato poi premiato da Telecom Italia con il Working Capital e 25mila euro, che hanno consentito ai fondatori (con Antonio anche Roberta Pellegrino, Federico Papa, Francesco Giacalone, Antonino Randazzo, Francesco Aronica e Salvatore Monello) di finalizzare la realizzazione del software ed aprire il sito dove ora è pubblicato il motore di ricerca: https://ludwig.guru/

FACEBOOK INCOMINCIA A TEMERE LINKEDIN ED INSTAGRAM



Con l'aggiornamento odierno dell'applicazione per dispositvi mobili, Facebook tenta di fidelizzare i propri iscritti, rinnovando l'interfaccia e la posizione dei comandi rendendola molto simile all'interfaccia dell'applicazione Instagram.

In effetti il menu di gestione del Social si è spostato dall'alto al basso della schermata principale. Ciò rende certamente minori gli spostamenti del dito dell'utente che ora può mantenere la mano in posizione, per reggere l'involucro dello smartphone, riuscendo così ad interagire con Facebook con il solo dito pollice.

La rete ha già ribattezzato con un neologismo il rinnovamento dell'app di Zuckerberg, definendo l'operazione di restyling come "l'instagrammazione" di Facebook.

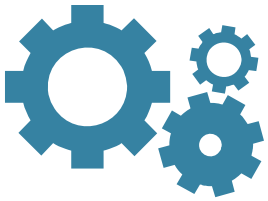
Così mentre in Italia il colosso dei Social Network cerca di riportare sulla propria piattaforma molti utenti che hanno iniziato a prediligere Instagram, in America ed in Canada Facebook tenta la concorrenza alla piattaforma Linkedin, con l'integrazione di nuove funzioni per la ricerca di lavoro.

Alle aziende infatti Facebook ha iniziato ad offrire pagine a pagamento orientate alla pubblicazione di annunci di lavoro, mirando a rendere più semplice il contatto tra offerta e candidati.

Gli utenti che vogliono candidarsi potranno visualizzare e trovare le offerte sul loro diario e nei loro segnalibri.

L'azienda clicca su un pulsante per aggiungere l'offerta alla propria pagina, trovandosi in una scheda in cui è possibile indicare la posizione che si sta cercando, la località, la paga, il tipo di contratto ed eventualmente integrare le caratteristiche che deve avere il candidato. Una volta che l'offerta di lavoro è stata pubblicata, sarà disponibile per 30 giorni e i candidati potranno mettersi in contatto con l'azienda direttamente attraverso l'app per smartphone, cliccando sul tasto Apply Now.

Software ed Utility



BullGuard IoT Scanner

BullGuard IoT Scanner è un tool online che consente di verificare eventuali falle di sicurezza nei dispositivi connessi ad internet. Utilizzabile per smartTV, videocamere di sicurezza, termostati, prese di corrente e lampade controllate via internet, web radio, elettrodomestici di nuova generazione che sfruttano l' IoT (Internet of Things), permette di accertare che questi oggetti siano a prova di hacker.

L'IoT ci permette di fare cose prima impossibili ma al tempo stesso pone nuove questioni relative alla sicurezza. Se ci sono falle nel software di questi dispositivi, un hacker potrebbe sfruttarle per violarli e prenderne il controllo. Potrebbe ad esempio accedere alle immagini della ip cam per sapere quando non siamo in casa e fare un furto, rubarci la password del WiFi, aprire le porte di casa e intrufolarsi a nostra insaputa e così via.

L'applicazione BullGuard sfrutta i dati open offerti dal motore di ricerca Shodan.io, il primo motore web per i dispositivi IoT, così se un dispositivo ha qualche falla di sicurezza verrà elencato nel motore di ricerca e l'applicazione lo individuerà.

Per avviare l'applicazione bisogna collegarsi al sito iotscanner.bullguard.com e cliccare sul collegamento Check if I am on Shodan. Se è tutto ok e non ci sono dispositivi accessibili da internet, altrimenti sarà utile effettuare un "deep scan" (controllo approfondito) per individuare anche i rimedi al problema riscontrato.

GOOGLE COMUNICA LA TUA POSIZIONE AI TUOI CONTATTI

Big G ha tirato fuori un nuovo asso dalla manica delle sue innovazioni tecnologiche.

Da oggi è possibile condividere la propria posizione geografica con i contatti della propria rubrica telefonica.

Grazie ai servizi del motore di ricerca e delle mappe del servizio Google Maps, dai dispositivi dotati di GPS e connessi ad internet, utilizzando l'app di Google Maps è possibile far tracciare i propri spostamenti ad uno, o ad altri, utenti contemporaneamente connessi a Google Maps.

Fino a poco tempo fa era possibile condividere la propria posizione in modo statico, ovvero si poteva inviare a qualcuno i dati gps della propria posizione in quell'istante. Con la nuova funionalità dell'app ora si può condividere la propria posizione in tempo reale, attivandola ed indicando i contatti a cui farla conoscere.

Nel menu dell'applicazione si può trovare il nuovo comando "Condividi posizione", una volta scelto, si potrà indicare per quanto tempo la posizione dovrà essere condivisa, o se la si vorrà poi disattivare manualmente, quindi selezionare le persone con cui condividerla.

Infine l'applicazione consente di decidere se visualizzare anche la posizione dei contatti a cui si invia il proprio link.

ANCHE I COMPUTER SI AMMALANO

Sono diverse le tipologie di virus che possono infettare i computer, conoscerli può aiutare a tarare opportunamente le difese e gli accorgimenti per evitarli.

Già nel 1949 John von Neumann dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente. Il concetto di programma auto-replicante trovò la sua evoluzione pratica nei primi anni '60 nel gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T chiamato "Core Wars", nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici.

Il termine virus venne adottato la prima volta da Fred Cohen (1984) della University of Southern California nel suo scritto Experiments with Computer Viruses (Esperimenti con i virus per computer), dove questi indicò Leonard Adleman come colui che aveva adattato dalla biologia tale termine. La definizione di virus era la seguente: "un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di sé stesso".

Ma il termine era già stato utilizzato prima. Nel 1972 David Gerrold scrisse un romanzo di fantascienza La macchina di D.I.O. (When H.A.R.L.I.E. was One), dove è presente una descrizione di un programma per computer chiamato VIRUS che adotta il medesimo comportamento di un virus.

Il primo malware della storia informatica è stato Creeper, un programma scritto per verificare la possibilità che un codice potesse replicarsi su macchine remote. Il programma chiamato Elk Cloner è invece accreditato come il primo virus per computer apparso al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata con lo scambio di floppy disk: il virus si copiava nel settore di boot del disco e veniva caricato in memoria insieme al sistema operativo all'avvio del computer.

Nel corso degli anni ottanta e nei primi anni novanta fu lo scambio dei floppy la modalità prevalente del contagio da virus informatici. Dalla metà degli anni novanta, invece, con la diffusione di internet, i virus ed i cosiddetti malware in generale, iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni.

Oggigiorno infatti con la rete internet, la posta elettronica, i router, i pen drive, i server web ed e-mail, le pagine web di siti e social network le diffusioni di virus informatici sono molto più rapide, avvengono da una parte all'altra del mondo e spesso vengono utilizzate per combattere guerre.

Pertanto qualsiasi dispositivo che abbia un sistema operativo ed è connesso ad Internet è potenzialmente a rischio di essere infettato da un virus. Consideriamo pure che la tecnologia dell'Internet of Thing (internet delle cose) ha portato la connessione alla rete globale in tantissimi dispositivi, quali: televisori, telecamere, automobili, apparecchi radio, dispositivi di telecontrollo dell'ambiente domestico o industriale, elettrodomestici, controllori automatici del traffico urbano, navale, ferroviario o aereo, ecc

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:

– una routine di ricerca, che si occupa di ricercare dei file adatti ad essere infettati dal virus e controlla che gli stessi non ne contengano già una copia, per evitare una ripetuta infezione dello stesso file;
– una routine di infezione, con il compito di copiare il codice virale all'interno di ogni file selezionato dalla routine di ricerca perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

Molti virus sono progettati per eseguire del codice estraneo alle finalità di replicazione del virus stesso e contengono dunque altri due elementi:

– la routine di attivazione, che contiene i criteri in base ai quali il virus decide se effettuare o meno l'attacco (es. una data, o il raggiungimento di un certo numero di file infetti);
– il payload, una sequenza di istruzioni in genere dannosa per il sistema ospite, come ad esempio la cancellazione di alcuni file o la visualizzazione di messaggi popup sullo schermo (gli adware sono malware che si specializzano nel far apparire banner pubblicitari su computer della vittima).

Le tipologie di Virus informatici, come per le specie biologiche, sono divise in macrofamiglie, ognuna con una sua peculiarità di infezione e diffusione e vengono classificati in base:
* all'ambiente di sviluppo,

– file virus, che a loro volta si dividono in:
+ parasitic virus;
+ companion virus;
+ virus link;
+ boot virus;
+ macro virus;
+ network virus

* alle capacità operative degli algoritmi: TSR virus, virus polimorfi, stealth virus,
* alle capacità distruttive
– innocui: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer;
– non dannosi: se comportano solo una diminuzione dello spazio libero sul disco, col mostrare grafici, suoni o altri effetti multimediali;
– dannosi: possono provocare problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file, modifica di file o apertura di applicazioni);
– molto dannosi: Causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema (formattazione di porzioni del disco, modifica dei parametri di sicurezza del sistema operativo, ...).

Riepiloghimo di seguito le definizioni fornite da Google e da WikiPedia per queste macrocategorie di virus informatici, che talvolta vengono anche utilizzati da hacker (genericamente operatore molto esperto, nda) e craker (o Black Hat Hacker – persona che si ingegna per eludere blocchi imposti da qualsiasi sistema informatico, nda) per ottenere l'accesso ai sistemi informatici presi di mira:

Adware: software scaricato, spesso in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per raccogliere informazioni sulle operazioni effettuate dall'utente e per visualizzare periodicamente messaggi pubblicitari non richiesti.

Keylogger: è uno strumento hardware o software in grado di effettuare lo sniffing della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato.

Malware: programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.

Ransomware: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.

Rogueware: anche noto come FraudTool (letteralmente "strumento di frode"), è una particolare categoria di malware che finge di essere un programma noto, o comunque non malevolo (ad esempio un Antivirus), al fine di rubare dati confidenziali o di ricevere denaro. Questi malware hanno anche, al loro interno, funzionalità di adware.

Rouge-AV o Rouge-Antivirus: il Rogue-AV, detto anche FakeAV, è un particolare Rogue che finge di essere un Antivirus: una volta installato nel computer, finge di trovare uno o più virus informatici e/o malware.

Rootkit: è una collezione di software, tipicamente malevoli, realizzati per ottenere l'accesso ad un computer o ad una parte di esso, che non sarebbe altrimenti possibile (per esempio un utente non autorizzato ad effettuare il login).

Spyware: software scaricato, spesso in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario.

Trojan: un trojan o trojan horse (in italiano Cavallo di Troia), nell'ambito della sicurezza informatica, indica un tipo di malware. Il trojan nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo.

Virus: è un programma o una sezione di codice caricato nel computer senza che il proprietario ne sia a conoscenza o lo abbia autorizzato. Alcuni virus causano solo fastidi, mentre la maggior parte è dannosa e ideata per infettare e prendere il controllo dei sistemi vulnerabili.

Worm: (letteralmente "verme") è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus ma, a differenza di questo, non necessita di legarsi ad altri eseguibili per diffondersi ma si diffonde spedendosi direttamente agli altri computer, ad esempio tramite e-mail o una rete di computer.

Non esiste un metodo generale per individuare un virus all'interno di un sistema. Le tecniche di rilevamento utilizzate dagli antivirus sono diverse: utilizzate contemporaneamente garantiscono un'ottima probabilità di rilevamento della presenza di un virus. In base alle tecniche di rilevamento usate, gli antivirus si distinguono in tre tipi:

* programmi di monitoraggio: mirano a prevenire un'infezione mediante il controllo di attività sospette (ad esempio, la richiesta di formattazione di un disco oppure l'accesso a zone privilegiate di memoria). Sono importanti perché rappresentano la prima linea di difesa (essi non rimuovono il virus; lo individuano e lo bloccano). Ma sono facili da bypassare attraverso la tecnica di tunneling.
* scanner: effettuano la ricerca dei virus attraverso due tecniche:
– il confronto tra le firme memorizzate in un database interno, con quelle, eventualmente, contenute nei file infetti;
– l'utilizzazione delle tecniche euristiche per i virus che sono cifrati o sconosciuti.
* programmi detection: utilizzano duniche:
– verifica dell'integrità: calcolano l'hash dei file da confrontare successivamente coi nuovi valori risultanti da un nuovo calcolo per verificare che i file non abbiano subito modifiche nel frattempo.
– tecniche euristiche: salva le informazioni sufficienti per ripristinare il file originale qualora questo venga danneggiato o rimosso da un virus

Ricordiamo infine che la scarsa conoscenza dei meccanismi di propagazione dei virus e il modo con cui spesso l'argomento viene trattato dai mass media favoriscono la diffusione tanto dei virus informatici quanto dei virus burla, detti anche hoax: sono messaggi che avvisano della diffusione di un fantomatico nuovo terribile virus con toni catastrofici e invitano il ricevente ad inoltrarlo a quante più persone possibile. È chiaro come questi falsi allarmi siano dannosi in quanto aumentano la mole di posta indesiderata e diffondono informazioni false, se non addirittura dannose.