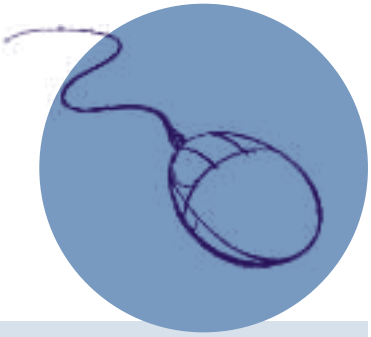


La Borsa *della* Spesa
Edizione 1.18

Doppioclick:
Riciclare uno smartphone per scienza e sicurezza

Se avete in casa uno smartphone che non usate più ma funziona ancora, ci sono due app che permettono di dargli nuova vita, per insegnare la scienza attraverso esperimenti e per creare un antifurto ultraportatile.

La prima si chiama Science Journal, disponibile per Android e iPhone; la seconda è Haven, ed è offerta solo per Android. Entrambe sono gratuite e usano lo smartphone in un modo ingegnoso e originale, sfruttando i suoi vari sensori incorporati (microfono, fotocamera, accelerometro, barometro, bussola e magnetometro).

Science Journal trasforma il telefonino in un piccolo laboratorio portatile: permette di misurare i livelli di rumore, le accelerazioni (per esempio in auto, sull'ottovolante o in ascensore), la luminosità, il magnetismo o la pressione (in montagna o in aereo) e registrare questi dati nel tempo: l'ideale per stuzzicare la mente di qualunque giovane aspirante scienziata o scienziato. I dati possono essere registrati, rappresentati graficamente e trasferiti ad altri dispositivi.

Haven, invece, permette di mettere in sicurezza una stanza, un oggetto o un cassetto: basta attivare l'app e il telefonino rileverà qualunque movimento nella stanza (tramite la fotocamera) e qualunque tentativo di spostare lo smartphone stesso. Se lo lasciate in un armadietto di cucina per scoprire chi ruba i biscotti, il suo microfono rileverà il rumore dell'apertura, il suo accelerometro ne percepirà le vibrazioni e la sua fotocamera farà una bella foto al ladro goloso. In albergo, sorveglierà la stanza per voi. Haven è abbastanza sensibile da accorgersi se qualcuno tenta di spegnerlo o scollegarlo dal caricabatteria. Se è connesso al Wi-Fi o alla rete cellulare, inoltre, vi spedirà un messaggio d'allerta in tempo reale insieme alla fotografia dell'intruso, per cui sarà utile anche se il ladro se lo porta via, se non altro per avvisarvi dell'avvenuta intrusione..

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 2.18

Doppioclick:
Trucchi per ridurre la dipendenza da smartphone

Gli smartphone sono progettati per creare dipendenza, ma se si conoscono le tecniche psicologiche usate dai progettisti delle app per farci passare sempre più tempo davanti ai loro piccoli schermi possiamo usarli senza esserne usati, come spiega su Vox.com Tristan Harris, che ha lavorato per Google come esperto di etica della progettazione e del design.

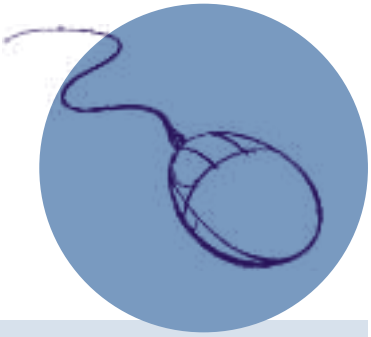
Harris propone quattro trucchi difensivi fondamentali. Primo: spegnere le notifiche automatiche. Ben vengano le notifiche delle chiamate o dei messaggi, perché vogliono dire che c'è una persona reale che vuole comunicare con noi. Ma molte app oggi creano un fiume di notifiche artificiali (per esempio "Mario è interessato a un evento vicino a te" o "a Piera piace questo video") per farci spendere più tempo a sfogliarle. Più tempo, infatti, per i produttori di queste app significa più soldi.

Secondo: mai trascinare verso il basso per aggiornare la schermata di un'app. Il trascinamento compulsivo è un trucco copiato (anche come gestualità) dalle slot machine per creare un ciclo di curiosità, azione e attesa per il risultato imprevedibile che allunga i tempi di utilizzo e quindi gli incassi. Basta aspettare e si aggiornerà automaticamente.

Terzo, molto drastico: togliere il colore. Le icone delle app usano colori caldi e vivaci per attirare l'attenzione (il pallino delle notifiche è rosso per questo, per esempio). Sull'iPhone, Impostazioni - Generali - Accessibilità - Scala di grigi produce uno schermo in bianco e nero che smetterà di assillare e chiamarci. È un ottimo sistema per far passare ai bambini la voglia di giocare con gli smartphone dei genitori.

Quarto, mettere nella schermata principale solo le app di utilità, come Maps, Calendario, Orologio o Calcolatrice e relegare ad altre schermate ogni app che offra lo "scorrimento infinito", ossia che proponga un pozzo senza fondo di contenuti nei quali perdersi, come Twitter, Facebook o Instagram.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 3.18

Doppioclick:
I trucchi dei ricattatori intimi: come difendersi

Lei è Véronique, lui Marco. Si sono incontrati su Omegle.com, un sito che permette di fare videochiamate via Internet con sconosciuti, gratuitamente, anonimamente e senza doversi iscrivere: un'attività molto diffusa soprattutto fra i giovanissimi, perché Omegle (come il rivale Chatroulette.com) è in apparenza popolato di belle ragazze molto disponibili. Ma le apparenze ingannano, e Marco se ne è accorto troppo tardi. Ha avviato con Véronique una conversazione in video che ben presto è diventata molto intima ed esplicita. Solo che Véronique in realtà non esiste: è lo pseudonimo di un truffatore che invece di mostrarsi all'interlocutore tramite la telecamerina del computer o del telefonino, come ha fatto Marco, trasmette al posto della propria immagine una registrazione di una ragazza molto disinibita che maneggia una tastiera. Il truffatore ha registrato tutto quello che Marco ha fatto durante la videochiamata e ora minaccia di mandare la registrazione alla polizia se Marco non gli manda parecchi soldi entro poche ore tramite Western Union, Moneygram o altri mezzi di pagamento. Il ragazzo, minorenne, è nel panico. Ho descritto un caso reale di ricatto via Internet che ho seguito di recente e di cui ho cambiato soltanto i nomi. Non è certo l'unico del suo genere: questo reato prospera anche in Svizzera, facendo leva sulla paura e sulla vergogna, che impediscono di chiedere aiuto ai genitori o alle autorità. La prevenzione è tutto, ma se il danno è fatto ci si può comunque difendere.

Il primo passo è non pagare, perché un pagamento non garantisce che il truffatore non chiederà altro denaro. Il secondo è rendersi conto che la minaccia di mandare il video in polizia è vuota, perché fare un video intimo del genere non è reato: la polizia non se ne farebbe nulla. Il terzo è rendere privato il profilo Instagram e nascondere l'elenco degli amici in Facebook, perché alcuni truffatori cercano sui social network gli amici della vittima per minacciare di mandare loro il video. In realtà non lo fanno quasi mai, specialmente se la vittima è minorenne, perché inviarlo significherebbe per loro commettere il reato di diffusione di pedopornografia. Il quarto e ultimo è troncare ogni contatto col truffatore: gli fa capire che non vedrà un soldo e quindi lascerà perdere, passando purtroppo alla prossima vittima.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 4.18

Doppioclick:
GDPR, cosa cambia per l'utente comune?

Il 25 maggio scorso è diventata applicabile la GDPR, la nuova serie di norme europee sulla protezione dei dati personali. Le aziende si stanno adoperando per mettersi in regola, ma cosa deve fare invece un utente privato che risiede in Svizzera?

Essendo la GDPR un regolamento dell'Unione Europea, verrebbe facile pensare che un utente svizzero non sia toccato, ma non è così se adoperano per esempio i servizi online di un'azienda dell'UE, come un social network o un negozio online, che è tenuto a gestire secondo il nuovo regolamento anche i dati delle persone fisiche che risiedono fuori dall'Unione.

Viceversa, un'azienda svizzera deve rispettare la GDPR se offre beni o servizi a persone residenti nell'Unione.

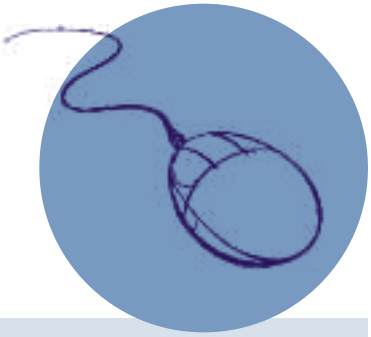
Uno dei primi effetti benefici della GDPR è la valanga di mail di aziende che chiedono il consenso a continuare a inviare informazioni: è un'occasione per eliminare le comunicazioni pubblicitarie indesiderate, perché basta che non rispondiamo alle richieste di consenso e le aziende che rispettano la GDPR smetteranno di mandarci queste mail. Per contro, se c'è per esempio una newsletter che vogliamo continuare a ricevere dobbiamo rispondere affermativamente alla richiesta di consenso.

Non dobbiamo fare nulla, invece, se gestiamo dati personali per attività esclusivamente personali e domestiche, che sono specificamente escluse dall'ambito della GDPR: quindi possiamo continuare a usare le nostre rubriche degli indirizzi e dei numeri di telefono di amici e parenti esattamente come prima.

La GDPR introduce anche maggiore trasparenza: abbiamo ora il diritto di sapere quali nostri dati vengono raccolti e di rettificarli, scaricarne una copia e farli cancellare.

È per questo che Instagram, Facebook e tanti altri servizi hanno attivato l'opzione di scaricamento di tutti i dati di un account, mentre Whatsapp ha scelto drasticamente di vietare l'accesso ai minori di sedici anni in Europa, Svizzera compresa, anche se non c'è alcun modo tecnico per far rispettare questo divieto.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 5.18

Doppioclick:
Braccialetto di fitness usabili per stalking

Usare i dispositivi di monitoraggio dell'attività fisica, dagli smartwatch ai braccialetti appositi come Fitbit o Polar, è molto utile per motivarsi e per tracciare i propri progressi. Ma a volte i dati raccolti da questi dispositivi possono esporci a rischi inattesi, per cui conviene imparare a impostare correttamente le app che li comandano.

Per esempio, molti di questi dispositivi tracciano la posizione dell'utente (geolocalizzazione) e la comunicano non solo all'azienda produttrice ma anche a chiunque voglia pedinarci. A volte siamo addirittura noi ad annunciare pubblicamente sui social network a che ora usciamo a correre e che percorso facciamo regolarmente, magari in tempo reale. Lo facciamo per competere con gli amici, o per annunciare al mondo le nostre imprese ginniche: ma abbiamo considerato che queste informazioni sono perfette per un ladro che volesse sapere quando siamo fuori casa, per un ex partner geloso o per un aggressore?

Di recente è emerso che app come Strava e Polar Flow consentono a chiunque di tracciare in massa i movimenti dei loro utenti se non si prendono precauzioni. Se ne sono accorti con imbarazzo i militari di vari paesi, i cui allenamenti rivelano i loro nomi e cognomi e i luoghi dove prestano servizio. Anche a livello privato, un malintenzionato può dedurre dove abitate semplicemente guardando il punto di partenza e di arrivo delle vostre corse.

Per fortuna i rimedi sono semplici, una volta che ci si è resi conto del problema: per prima cosa, non iscrivetevi usando il vostro vero nome e cognome, non mettete il vostro volto come immagine del profilo e non usate l'opzione di iscrivervi tramite Facebook (che offre a tutti il vostro nome e l'elenco dei vostri amici). Poi impostate il vostro profilo nell'app di fitness in modo che i dati principali (orari e geolocalizzazione) non siano pubblicamente consultabili e disattivate l'opzione di condividere le vostre attività atletiche sui social network.

Certo, significa non poter partecipare a gare online e non poter fare vanto pubblico della vostra forma fisica, ma evitare le molestie di un aggressore o un furto in casa è più importante. E per tener traccia dei propri progressi è sempre possibile usare cronometro, carta e penna, anche nell'era delle app.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 7.18

Doppioclick:
Febbre da Fortnite

Fortnite è un videogioco popolarissimo che appassiona i giovani giocatori e tormenta i loro genitori che non riescono a staccare i figli dallo schermo. Ma è anche una miniera d'oro per i truffatori: nel gioco, infatti, si possono fare acquisti virtuali che si pagano con denaro reale (spesso tramite la carta di credito dei genitori) e ottenere ricompense in moneta virtuale (V-Buck), e quindi gli account che accumulano questi acquisti e premi vengono rubati per rivenderli.

Se volete far bella figura con i vostri figli o nipoti, consigliate loro di attivare in Fortnite l'antifurto, ossia la cosiddetta "autenticazione a 2 fattori": basta andare su https://Epicgames.com/2FA e seguire le istruzioni. Da quel momento solo il telefonino, tablet, computer o console di gioco autenticato potrà accedere all'account; nessun ladro potrà accedervi, neppure se scopre la password del giocatore.

Un'altra raccomandazione di prudenza, più difficile da far accettare a chi è preso dalla febbre del gioco ma comunque importante, è non installare versioni piratate o altre app che promettono di barare (le cosiddette "cheat"): sono spesso esche per imbrogliare, rubare account o infettare computer o smartphone. Meglio starne alla larga e associare all'account una carta di credito prepagata invece di quella tradizionale.

Per i genitori c'è anche l'assillo di dover interrompere le sessioni di gioco dei figli, che non si accorgono del tempo che trascorrono incollati allo schermo di Fortnite. Per chi ha un iPhone o iPad recente e aggiornato ci sono per fortuna delle soluzioni integrate, come Tempo di Utilizzo (nella sezione Impostazioni), che permettono di definire una fascia oraria e un limite di tempo che valgono per tutti i giochi. Questa impostazione è bloccabile tramite un PIN e può anche essere estesa a tutti i dispositivi Apple di famiglia. Per Android c'è l'app Google Family Link, che funziona in modo analogo.to!

PAOLO ATTIVISSIMO