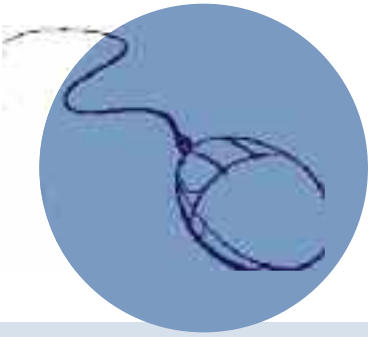


La Borsa *della* Spesa
Edizione 1.16

Doppioclick:
Realtà virtuale, promettente moda del momento

Si prende lo smartphone, lo si inserisce in un economico visore da applicare sugli occhi e ci si trova di colpo immersi in un mondo alternativo, tridimensionale e iperrealistico. Si possono vedere i film in 3D e guardare gli appositi video su Youtube con un effetto sconcertante: quando si sposta la testa a destra, a sinistra, in alto o in basso l'immagine si sposta in modo corrispondente. Sembra di essere circondati dallo schermo in tutte le direzioni.

Questa è la cosiddetta "realtà virtuale": una tecnologia usata da anni con successo nell'industria aerospaziale per addestrare astronauti e piloti e nei musei per ricostruire ambienti inaccessibili o non più esistenti. Ora viene offerta in versione per consumatori a prezzi molto variabili: da pochi franchi per il modello Cardboard di Google (con un visore fatto letteralmente di cartone) a centinaia per Rift di Oculus o Gear VR di Samsung.

È la moda informatica del momento e gli appassionati di videogiochi non vedono l'ora di poterla usare per giocare in modo ancora più realistico. Ma bisogna fare attenzione per non rischiare di buttar via il proprio denaro. Per avere un risultato accettabile nei videogiochi, per esempio, occorre procurarsi uno smartphone recentissimo, molto potente e con uno schermo che non solo dev'essere ad altissima definizione (un Quad HD, se possibile) ma deve avere uno spazio ridottissimo tra i pixel (i puntini che formano l'immagine), altrimenti si otterrà un fastidioso "effetto zanzariera": sembrerà di guardare il mondo attraverso un retino, rovinando l'illusione visiva. Per i modelli di punta serve anche un personal computer estremamente potente. Il visore in sé, insomma, è solo una piccola parte della spesa necessaria. Prima di fare l'investimento, inoltre, conviene fare una prova pratica con un impianto altrui: a molti utenti, infatti, la realtà virtuale crea fastidio e nausea anche con i sistemi più moderni e potenti a causa del disorientamento della percezione: il corpo e l'orecchio interno dicono che si è fermi ma gli occhi dicono tutt'altro. La sensibilità a questa dissonanza percettiva varia enormemente da persona a persona. Inoltre i visori sono piuttosto pesanti e lasciano respirare poco il viso, per cui è difficile guardare un intero film o videogiocare a lungo senza uscirne indolenziti e accaldati. Ma per i fortunati che non soffrono la nausea, la realtà virtuale ha un "effetto wow" garantito.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 2.16

Doppioclick:
Carte di credito e videogiochi, abbinamento pericoloso

Ricevere una bolletta di 2300 franchi per aver giocato a FIFA con la Playstation non sembra possibile, ma è solo un esempio (tratto dalla realtà ticinese) dei rischi che si corrono se si registrano i dati della propria carta di credito nella memoria apparentemente sicura delle console di gioco più moderne, dei tablet e degli smartphone. Molti dei videogiochi disponibili su questi dispositivi hanno infatti gli "acquisti in-app": si spendono soldi veri per ottenere privilegi o oggetti immaginari (per esempio superpoteri, armi, giocatori o gemme). Se non si prendono precauzioni, il giocatore non si rende conto di quanto sta spendendo e le cifre in gioco salgono in fretta. Sono inoltre frequenti i furti delle password che proteggono gli account dei giocatori: il ladro gioca e fa acquisti virtuali addebitandoli sulla carta di credito del derubato.

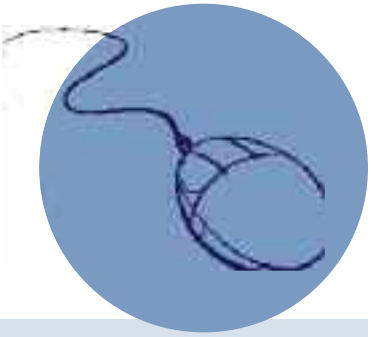
Contestare gli addebiti per chiederne il rimborso causa altri problemi: molte reti di gioco non restituiscono denaro ma offrono buoni acquisto (è previsto dal contratto che non legge mai nessuno) e in alcuni casi bloccano il giocatore frodato per vari mesi. In altre parole, il consumatore ha sempre torto.

In queste condizioni l'unica strada percorribile è la prevenzione: il primo passo è registrare una carta di credito prepagata invece di una normale oppure usare i buoni acquisto che si possono ottenere via Internet o sotto forma di tessera in molti punti vendita, in modo da limitare l'importo possibile del danno in caso di frode o abuso. Il secondo è attivare gli avvisi via SMS per essere allertati subito se avvengono transazioni non autorizzate.

Conviene poi cambiare password periodicamente e non affidarla ad amici, come invece si fa spesso, e avere password complesse e non ovvie. Alcune reti di gioco, come Xbox Live e Steam, hanno una protezione ulteriore chiamata "verifica in due passaggi", che è poco usata ma è utilissima. Anche tenere d'occhio la mail è importante, perché eventuali acquisti fraudolenti verranno segnalati da un messaggio email; al tempo stesso, via mail possono arrivare finti messaggi che sembrano provenire dalle reti di gioco ma provengono da truffatori che invitano a cliccare su un link con la scusa di verificare la password e in realtà la rubano.

Tutto troppo complicato? Ci sono anche console più semplici, e comunque si può sempre giocare a pallone nella vita reale ed evitare tutti questi problemi.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 3.16

Doppioclick:
Antivirus necessari ma non sufficienti

Ormai è probabilmente chiaro a tutti che chi ha un computer deve attrezzarsi con un buon antivirus: è meno chiaro che questa necessità riguarda non solo i computer dotati di Microsoft Windows ma anche quelli della Apple (che contrariamente a un mito molto diffuso sono vulnerabili ai virus informatici). È ancora meno diffusa la consapevolezza che anche i tablet e gli smartphone dotati di Android (praticamente tutte le marche tranne Apple e Microsoft/Nokia) hanno seriamente bisogno della protezione di un antivirus: del resto, sono computer a forma di telefono e quindi hanno le stesse fragilità dei computer tradizionali e per di più hanno accesso diretto al nostro portafogli tramite la bolletta, per cui sono diventati un bersaglio preferito dei criminali informatici. Molti antivirus vengono incontro all'utente offrendo un pacchetto unico che aiuta a proteggere tutti i computer, tablet e smartphone di una famiglia o di un'azienda.

Lo spazio occupato dall'antivirus sul disco rigido o nella memoria del dispositivo non è più un problema, vista la capienza dei dischi e delle memorie di oggi, ma alcuni antivirus rallentano molto il funzionamento dei computer perché esaminano automaticamente ogni dato e ogni messaggio che viene scaricato e ogni documento che viene aperto: di solito, comunque, questi automatismi sono disattivabili almeno per i file più grandi (video e musica, per esempio) che causano grossi rallentamenti. Va ricordato, in ogni caso, che gli antivirus non sono una difesa perfetta: credere di poter scaricare e installare qualunque app trovata nei bassifondi di Internet o di poter aprire qualunque allegato senza pericoli perché tanto ci protegge l'antivirus è una ricetta per un disastro garantito. La prudenza e il buon senso non vanno messi nel cestino: per esempio, le app che promettono falsamente gemme gratis in Clash of Clans stanno facendo molte vittime fra gli utenti di smartphone più giovani.

Conviene creare nel computer un utente limitato per navigare? Senz'altro, perché impedisce ai virus di infettare le applicazioni. Purtroppo, però, molti virus moderni attaccano e bloccano i dati dell'utente, che sono spesso insostituibili, e poi chiedono un riscatto per rilasciarli. Un utente limitato non previene questi attacchi. Le applicazioni infette si possono sempre reinstallare: le nostre foto o i nostri documenti no. Per proteggere i dati più preziosi è meglio fare prevenzione, copiandoli periodicamente dal computer, tablet o smartphone a un altro dispositivo, come un disco esterno o una chiavetta USB.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 4.16

Doppioclick:
Dubbi e paure su consumi e emissioni dei router Wi-Fi

I router Wi-Fi, ossia gli apparecchi forniti da Swisscom, Sunrise, Cablecom e altri operatori per diffondere senza fili la connessione Internet in casa a computer, tablet, smartphone, televisori e altri dispositivi sono diffusissimi e spesso ci si preoccupa per i loro consumi e per la loro possibile nocività. Vale la pena, per esempio, disattivarne le trasmissioni di notte?

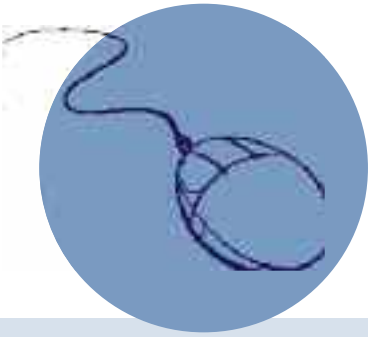
Sul fronte dei consumi di energia elettrica, i principali router Wi-Fi consumano molto poco rispetto a altri elettrodomestici che restano anch'essi permanentemente accesi, come frigoriferi o congelatori. Inoltre, secondo Svizzeraenergia.ch, spegnere soltanto la sezione Wi-Fi dei router non riduce significativamente i consumi di questi dispositivi: un vero risparmio si avrebbe spegnendoli completamente, ma questa è un'opzione sconsigliata da molti operatori Internet perché può causare malfunzionamenti. Non va dimenticato, inoltre, che lo spegnimento completo interrompe anche il servizio telefonico se si ha un contratto Internet che include la telefonia, ed è quindi consigliato soltanto in caso di assenze prolungate. In alternativa, molti router recenti, specialmente quelli combinati che offrono anche servizi TV e radio (set top box), hanno modalità di risparmio energetico intensivo che si possono attivare automaticamente usando le istruzioni dei vari operatori Internet, raccolte da Svizzeraenergia.ch presso tinyurl.com/router-energia.

Per quanto riguarda le emissioni dei dispositivi Wi-Fi e in particolare dei router, secondo l'Ufficio federale della sanità pubblica non emergono rischi sanitari attribuibili alle normali reti senza fili, che per le loro deboli potenze d'emissione sono al di sotto della soglia d'interesse dell'ordinanza sulla protezione dalle radiazioni non ionizzanti (ORNI).

Secondo l'Organizzazione Mondiale della Sanità, poi, non c'è correlazione fra i sintomi di coloro che si dichiarano affetti dagli apparati Wi-Fi e l'attività degli apparati stessi. Nei test, i soggetti non riescono a distinguere le emissioni elettromagnetiche reali da quelle che credono di subire, per cui si sospetta che la causa dei sintomi sia altrove.

Per maggiore serenità personale si può comunque ridurre facilmente la propria esposizione non solo spegnendo il trasmettitore se e quando possibile ma anche adottando semplici schermature e tenendo conto del fatto che già a 20 cm dall'antenna il segnale è 10 volte più debole del valore limite e a un metro è addirittura 40 volte più debole (tinyurl.com/ufsp-wlan).

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 5.16

Doppioclick:
Un libro-guida per internauti ticinesi (e non solo)

Tre firme ticinesi per colmare una lacuna sentita da molti genitori: un libro che spieghi Internet in termini di tecnologia, pedagogia e diritto con specifico riferimento alla realtà ticinese. Alessandro Trivilini (informatico e ricercatore alla Supsi), Ilario Lodi (responsabile di Pro Juventute Ticino) e Gianni Cattaneo (avvocato, docente di diritto dell'informatica) hanno riunito le proprie competenze per scrivere "Genitori nella Rete", libro edito da Armando Dadò Editore (Genitorinellarete.ch). Il libro è stato pubblicato nel 2014, ma è ancora perfettamente attuale oltre che unico nella sua specificità.

I suoi consigli strettamente informatici sono preziosi, anche se talvolta un po' impegnativi da decifrare per un lettore alle prime armi, mentre la parte giuridica, strettamente riferita alla normativa svizzera, rivela con linguaggio chiaro aspetti ben poco conosciuti e per nulla intuitivi, come i reali diritti e doveri dei genitori di un minore che si affaccia a Internet con il computer o lo smartphone. Per esempio, è legale per un genitore leggere la mail personale di un figlio minorenne? La risposta corretta non è ovvia. I riferimenti di legge sono accompagnati da esempi concreti e consigli pratici su diritto d'autore, sicurezza degli acquisti, protezione della sfera privata e della reputazione, sexting, pornografia, videogiochi violenti, cyberbullismo e molti altri temi fondamentali, spesso fraintesi dagli utenti.

La parte pedagogica si articola su una serie di esercizi di riflessione per genitori che aiutano a capire come un figlio vive Internet e l'uso dello smartphone e dei social network in modo radicalmente diverso da un adulto e portano a soluzioni basate più sul dialogo e l'educazione che sulla tecnologia e le proibizioni, senza mai perdere di vista le grandi, irrinunciabili opportunità di crescita, di conoscenza e di reale socializzazione offerte dai dispositivi digitali che si affacciano a Internet, se usati con competenza e buon senso.

Paolo Attivissimo

La Borsa *della* Spesa
Edizione 6.16

Doppioclick:
Pokémon Go, occhio agli acquisti e alle app-truffa

L'enorme popolarità di Pokémon Go ha scatenato un'orda di imitatori, per cui nell'App Store di Apple e in Google Play per i dispositivi Android si trovano moltissime app dal nome molto simile a quello ufficiale (che è Pokémon Go di Niantic, Inc.). Quasi tutte queste app imitatrici sono gratuite e promettono trucchi e consigli per giocare meglio, e così molti pensano che non ci sia pericolo nel provarle. Purtroppo non è così: molte di queste app quasi omonime bombardano gli utenti con pubblicità inadatte ai bambini o rubano dati personali, come indirizzi di casa, rubriche o localizzazioni, per rivenderli.

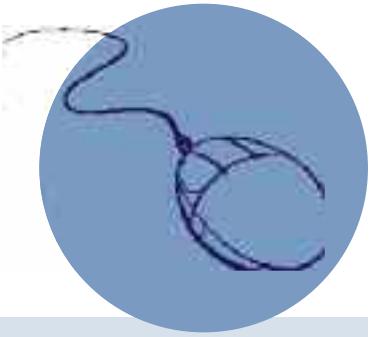
Ci sono poi delle app per Pokémon che si trovano al di fuori di App Store e Google Play, ma è meglio lasciarle perdere anche se sembrano identiche all'originale: se non sono presenti nei negozi ufficiali ci sarà pure un motivo. Infatti queste app "esterne" di solito sono delle trappole, perché possono farti fare telefonate o mandare SMS di nascosto, causando addebiti ingenti sulla bolletta. Parte del costo della telefonata finisce nelle tasche dei truffatori che hanno creato l'app.

Un caso particolarmente pericoloso è dato dalla versione per Windows di Pokémon Go, che in realtà non è stata distribuita dai creatori originali del gioco: è infatti una versione falsa, che blocca con una password complicatissima tutti gli accessi ai documenti digitali presenti nel computer e chiede un riscatto in denaro per rivelare la password di sblocco. Si tratta insomma di un cosiddetto ransomware, come quelli che di solito colpiscono le aziende bloccandone l'attività informatica.

I criminali informatici hanno creato tutte queste app truffaldine perché sanno che i giocatori di Pokémon Go sono molto spesso dei bambini e quindi sono vittime più facili da ingannare. L'unica difesa è limitarsi a usare l'app originale, evitando tutte le altre; per chi ha figli è opportuno spiegare loro il pericolo e impostare il loro smartphone in modo che non possano installare app senza il consenso di un genitore.

Non va dimenticato, infine, che anche l'app originale ha delle insidie: consente infatti di acquistare monete virtuali che costano fino a 100 franchi (reali), per cui conviene disabilitare gli "acquisti in-app" nelle impostazioni dello smartphone.

Paolo Attivissimo



La Borsa *della* Spesa
Edizione 7.16

Doppioclick:
WhatsApp prende i vostri dati e li passa a Facebook

Sorpresa: da fine settembre scorso WhatsApp passa automaticamente a Facebook vari dati personali che permettono a Facebook di identificarvi meglio. Per esempio, se usate WhatsApp e avevate rifiutato di dare a Facebook il vostro numero di telefonino, ormai Facebook se l'è preso, insieme ad altre informazioni, a meno che abbiate esplicitamente rifiutato questa condivisione (cosa che si poteva fare solo fino al 25 settembre).

Questo passaggio di dati fra WhatsApp e Facebook è stato deciso perché Facebook ha comprato WhatsApp nel 2014 per circa 19 miliardi di dollari e ora vuole monetizzare il proprio investimento, così come ha fatto con Instagram, acquisita nel 2012.

Questa novità significa che è facile rivelare inavvertitamente la propria attività privata su questi social network. Per esempio, se usate Facebook con uno pseudonimo, come fanno in molti, e adoperate anche WhatsApp, ora c'è il rischio che i vostri conoscenti possano scoprire il vostro pseudonimo su Facebook, perché adesso è associato al vostro numero di telefonino e quindi Facebook può consigliare come nuovo amico il vostro profilo segreto a chi vi conosce. Questo succede già, per esempio, fra Facebook e Instagram, dove capita spesso di vedere la notifica "Il tuo amico di Facebook (nome e cognome) è su Instagram come (pseudonimo)" che smaschera le identità nascoste dei conoscenti.

Facebook è molto reticente su quali dati specifici di WhatsApp vengano condivisi: per ora si sa che includono, oltre al numero di telefonino, il tipo di smartphone usato (iPhone o Android), le dimensioni dello schermo e l'orario dell'uso più recente di WhatsApp, ossia dati molti utili a Facebook per fare pubblicità mirata e profilare le abitudini degli utenti. Purtroppo l'unico modo per evitare questa condivisione ficcanaso è smettere di usare WhatsApp, per esempio passando ad app simili come Signal o Telegram.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 8.16

Doppioclick:
Il virus che formatta l'iPhone è una bufala, però...

Il recente allarme diffuso soprattutto tramite WhatsApp, secondo il quale esisterebbe un video chiamato "La danza di Hillary" che formatta il telefonino e sarebbe stato annunciato dalla BBC è una bufala totale. Si tratta di una variante di un altro appello-bufala, a proposito di un video intitolato "La danza del Papa", diffuso mesi fa e altrettanto fasullo. Ma anche se non esistono video capaci di formattare i telefonini e quindi non bisogna diffondere questi falsi allarmi, ci sono realmente dei video e delle immagini che sono in grado di paralizzare o danneggiare uno smartphone e in particolare un iPhone.

Poche settimane fa Apple ha segnalato che è effettivamente possibile prendere il controllo di un iPhone non aggiornato semplicemente inviandogli un'immagine appositamente confezionata. Ancora più recentemente alcuni ricercatori di sicurezza informatica hanno scoperto l'esistenza di un brevissimo video, intitolato a volte "Honey", che è in grado di mandare in "crash" un iPhone dopo qualche istante, costringendo l'utente a un riavvio forzato. Per effettuare il riavvio si premono contemporaneamente il tasto di accensione e quello di abbassamento del volume per dieci secondi, nel caso di un iPhone 7; per i modelli precedenti occorre premere insieme il tasto di accensione e il tasto Home.

Il rimedio, di solito, è aggiornare il telefonino alla versione più recente del suo software di gestione (in questo caso iOS), che corregge il difetto, e in generale prevenire il rischio evitando di scaricare e aprire video o immagini di dubbia provenienza.

Distinguere un allarme vero da uno falso è abbastanza semplice: quelli veri hanno sempre una fonte tecnica di riferimento ben precisa (per esempio un link a un avviso specifico sul sito della Apple, nei casi citati qui). L'indicazione generica "l'ha annunciato la BBC" è un sintomo di bufala; inoltre non bisogna basarsi sul nome del video o dell'immagine per fidarsi o meno.

PAOLO ATTIVISSIMO