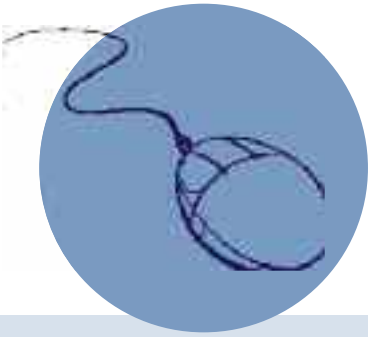


La Borsa *della* Spesa
Edizione 1.11

Doppioclick: i pensierini via mail fanno male?

I messaggi di e-mail che allegano documenti Word o presentazioni PowerPoint per diffondere storie umoristiche, messaggi politici, allarmi o pensieri profondi sull'esistenza, l'amore e l'amicizia sono una piaga di Internet che è particolarmente difficile debellare e che preoccupa molti utenti.

L'angoscia più diffusa è che questi messaggi contengano virus informatici o altri rischi di sicurezza, ma in realtà questo è un caso raro: i danni sono in genere di altro tipo.

Questi allegati, infatti, contribuiscono a intasare Internet e i computer. Una comune presentazione PowerPoint di questo tipo (frasi con alcune immagini di sfondo) equivale ad alcune migliaia di e-mail di puro testo. Di conseguenza, se chi la riceve ha una connessione lenta (per esempio tramite la rete cellulare), scaricarla costa tempo e probabilmente anche denaro. Una volta scaricata, inoltre, se non viene cancellata occupa posto nel computer.

Talvolta lo scaricamento si effettua invano, perché l'allegato è in un formato che non si può leggere perché non si possiede il programma corrispondente. Non tutti hanno sul computer l'ultima versione di Microsoft Word e PowerPoint, e oggi molti utenti leggono la mail da telefonini o altri dispositivi che non possono visualizzare allegati di questo tipo.

Alcuni di questi allegati, inoltre, citano nomi di presunti garanti e li associano a falsi allarmi, perpetuando il disagio di persone spesso coinvolte per errore in vere e proprie catene di Sant'Antonio diffamatorie o ingannevoli.

Dal punto di vista tecnico si può impostare nel computer o nella casella di posta un filtro che blocchi o posticipi lo scaricamento di tutti gli allegati che superano una certa dimensione e permetta di scaricare solo quelli che interessano realmente. Successivamente si possono cancellare dal computer gli allegati non più necessari. Il vero problema è che questi pacchetti di filosofia spicciola digitalizzata ci arrivano dagli amici, ai quali è imbarazzante dire che si è rifiutato un loro messaggio mandato in buona fede e spiegare che la stessa informazione poteva essere spedita come testo semplice e risultare utile e gradita lo stesso (anzi, di più). Per questi problemi, ahimè, non c'è rimedio informatico.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 2.11

Doppioclick: WiFi, paure per salute e sicurezza

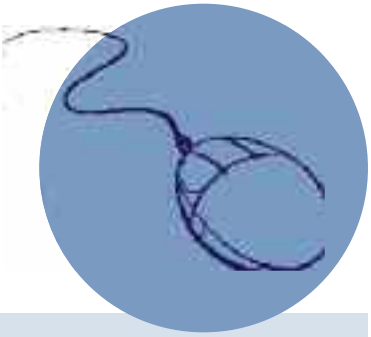
Il WiFi, l'antennina che diffonde Internet senza fili in casa, in ufficio e nei luoghi pubblici, è una grande comodità: evita la posa di cavi e consente di accedere alla Rete ad alta velocità anche con i telefonini predisposti. Ma c'è chi giustamente si pone il dubbio che le onde radio emesse dagli apparecchi WiFi possano essere nocive per la salute, soprattutto in caso di esposizione prolungata.

Secondo le ricerche pubblicate congiuntamente dall'Ufficio federale della sanità pubblica, dall'Ufficio federale delle comunicazioni e dall'Ufficio federale dell'ambiente, tutti questi apparati hanno emissioni ampiamente al di sotto dei limiti di sicurezza. Il loro campo elettrico non supera il 10% del valore limite già a venti centimetri dall'antenna e oltretutto diminuisce rapidamente all'aumentare della distanza: a un metro è già sceso al 2,5%. Non ci sono, per ora, documentazioni scientifiche di effetti nocivi chiaramente correlati a questi dispositivi, e la ricerca si scontra con il fatto che le emissioni WiFi avvengono in un ambiente dove ci sono emissioni ben più potenti, come quelle delle reti telefoniche mobili. In altre parole, se si vive in una zona coperta dal segnale cellulare e si usa assiduamente il telefonino, preoccuparsi per il WiFi è come preoccuparsi di diventare sordi per via della radio accesa quando si lavora in una segheria.

Si può comunque ridurre ulteriormente l'esposizione con semplici accorgimenti: per esempio, collocare l'antenna WiFi lontano da scrivanie o altre posizioni occupate a lungo, accendere l'apparato solo quando lo si usa e tenere lontano dal corpo i computer con antenna WiFi integrata quando si usa la connessione senza fili. Alcuni modelli possono regolare la propria potenza e quelli che usano lo standard "g" hanno un'emissione elettromagnetica inferiore.

La sicurezza informatica del WiFi è invece un problema molto reale. Il segnale radio WiFi è intercettabile e quindi si presta a intrusioni e furto di password e dati personali: va protetto attivando le apposite funzioni di cifratura (WPA2 o WPA, altrimenti WEP) e usando una password lunga e non intuitiva. È opportuno attivare il filtro sui "MAC Address" (un numero di serie che identifica ogni apparato di rete), in modo da consentire l'accesso solo ai singoli dispositivi autorizzati, cambiare e nascondere l'identificativo della rete (SSID) e comunque spegnere gli apparati WiFi quando non vengono usati, coniugando così salute, sicurezza e risparmio.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 3.11

Doppioclick: iPhone o Android, scelta difficile

I mercato degli smartphone, i telefonini evoluti in grado di gestire anche e–mail e Internet, è oggi in mano a tre grandi rivali: Apple (iPhone), Google (attraverso Android) e RIM (Blackberry), con poco meno del 30% a testa. Windows Phone, quarto contendente, è ampiamente staccato (10%). Mentre il mercato professionale si è orientato fortemente verso i modelli Blackberry, ben integrati nei servizi aziendali, molti consumatori sono indecisi principalmente fra Apple e Android.

Entrambi hanno pro e contro e non c'è una soluzione unica per tutti. Al livello più semplice, i due concorrenti si distinguono perché Apple offre sostanzialmente un solo modello (con capienza di memoria differente), mentre Android è disponibile in varie versioni e su una rosa molto ampia di telefonini di diversi fabbricanti con prezzi estremamente variabili. Per esempio, chi vuole un telefonino con una tastiera vera e propria oppure uno schermo più grande o più piccolo non lo troverà da Apple. Per contro, la standardizzazione dell'iPhone intorno a un modello unico semplifica la scelta e lo rende meglio accetto nelle aziende perché diventa più facile da gestire.

Per gli utilizzatori intensivi dei servizi Internet e di navigazione GPS, la batteria non rimovibile e non sostituibile dell'iPhone potrebbe risultare penalizzante, anche se di norma nelle zone dove la rete cellulare è capillare dura comunque un'intera giornata; i telefonini Android permettono invece all'utente di cambiare batteria. Apple non consente di espandere la memoria dell'iPhone, mentre molti dispositivi Android hanno una memoria espandibile e rimovibile che facilita il caricamento di dati (musica, video e documenti). La dipendenza dello smartphone da un computer è più spiccata nell'iPhone che nei cellulari Android, che però necessitano di un account gratuito Google per gran parte delle proprie funzioni. Apple non supporta la tecnologia Flash usata da molti siti per la grafica e i video; Android sì, ma al prezzo di un maggior consumo di batteria.

Alla fine, per molti utenti il criterio fondamentale di scelta è costituito dalle "app", ossia dai programmi installabili sullo smartphone (gratuitamente o a pagamento) per fargli fare le cose più disparate: giochi, contabilità, misurazioni e calcoli scientifici, musica. Se l'app di cui si ha bisogno (o un suo equivalente) non è disponibile, la scelta fra Android o iPhone diventa forzata. Conviene quindi valutare prima di tutto cosa si intende fare con il proprio smartphone.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 4.11

Doppioclick: PlayStation, il furto di dati non è un gioco

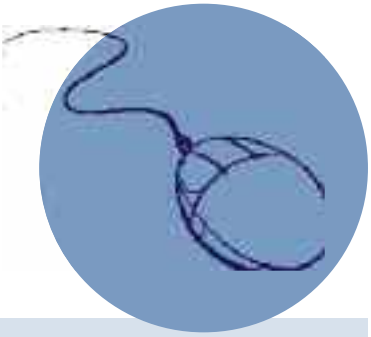
Il recente furto di cento milioni di dati personali di giocatori di PlayStation, sottratti alla Sony attraverso una serie di falle nella sicurezza della rete di gioco PlayStation Network (PSN), e la conseguente sospensione delle attività di gioco online per più di tre settimane hanno suscitato non solo scalpore e arrabbiature da parte degli acquirenti frustrati ma anche preoccupazione per il rischio di truffe legate all'abuso dei dati personali. Soprattutto hanno messo in evidenza che oggi il videogame su Internet non è più una cosa da prendere alla leggera: i suoi dati vanno custoditi con la stessa attenzione dedicata ai dati bancari.

Non è un problema esclusivo di Sony: tutte le reti di gioco hanno password, indirizzi e borsellini elettronici nei quali sono depositati crediti o forme di denaro equivalenti, e alcune (come il PlayStation Network) custodiscono i codici delle carte di credito degli utenti. Farsi sottrarre la password di un account di gioco significa perdere tutto questo e anche l'investimento di tempo fatto per raggiungere un certo obiettivo o livello nel gioco. Esiste addirittura un vero e proprio mercato nero degli account rubati, che vengono smerciati in cambio di denaro vero. Il danno economico di un account di gioco sottratto è quindi assolutamente reale e tangibile.

Chi è utente del PSN e vi ha usato una carta di credito farà dunque bene a sorvegliare il proprio estratto conto e a diffidare di qualunque richiesta di verifica dei dati che arrivi via mail o compaia su Internet, anche se Sony ne è il mittente, perché il mittente è facilmente falsificabile e queste richieste fasulle vengono usate regolarmente dai truffatori di Internet per carpire password e codici di carte di credito. Gli unici avvisi legittimi sono quelli che arrivano direttamente sulla PlayStation attraverso il Network.

Anche chi non ha usato carte di credito sulla rete Sony deve fare attenzione. Probabilmente, infatti, la password usata sul PSN è la stessa usata altrove, e siccome la password PSN è da considerare compromessa insieme al proprio indirizzo di e-mail, nome e cognome, data di nascita e indirizzo postale farà bene a cambiare password, i malfattori tenteranno di usare la password PSN per entrare nella mail, in Facebook o negli altri servizi Internet dell'utente. Conviene quindi cambiare anche le password degli altri servizi online se sono simili o uguali a quella usata sul PSN.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 5.11

Doppioclick: eBook, libri digitali comodi ma incompatibili

Quanto pesa la carta! Scegliamo un paio di libri da portare in vacanza e abbiamo aggiunto un chilo alla valigia. Immaginate ora di poter portare con voi centinaia di libri in meno di trecento grammi. Immaginate di poter leggere subito l'ultimo successo editoriale o il giornale di oggi senza andare in edicola o in libreria e senza attendere che arrivi per posta. Questa è la promessa degli e-book, i libri digitali, e dei loro dispositivi di lettura.

Tutti i grandi nomi dell'informatica e dell'editoria offrono e-book e lettori portatili, da Amazon a Google a Samsung a Sony, ma districarsi nelle opzioni non è facile. In teoria gli eBook si possono leggere anche sui telefonini evoluti, sui computer o sui tablet come l'iPad usando i programmi appositi, ma se intendete leggere molto e stando all'aperto o in ambienti fortemente illuminati conviene acquistare un lettore dedicato (reader), il cui schermo è leggibilissimo anche in piena luce (anche se per ora è in bianco e nero, con poche costose eccezioni).

Anche il peso e l'autonomia della batteria sono importanti, e i reader dedicati vincono a mani basse: qualche etto e durate che si misurano in settimane.

Poi c'è da scegliere fra tipi di connessione per scaricare libri e giornali: alcuni reader dipendono da un computer separato, altri usano le reti Wifi e altri ancora possono accedere gratuitamente alla rete telefonica cellulare (anche all'estero).

L'offerta di pubblicazioni digitali è ampia, anche in italiano: molti classici sono gratuiti e i libri recenti costano di norma meno dell'equivalente cartaceo. Purtroppo, però, i vari produttori ed editori usano formati spesso incompatibili. Un libro digitale per il lettore Kindle di Amazon può risultare illeggibile su un dispositivo Sony e viceversa. A volte il libro desiderato non è disponibile per uno specifico reader. In alcuni casi si può risolvere il problema usando programmi gratuiti di conversione, come Calibre o Kindlegen, ma i libri sono spesso protetti da lucchetti digitali anticopia (DRM) che ostacolano queste conversioni e legano il libro al dispositivo: se cambiate marca, rischiate di perdere la vostra biblioteca. La carta pesa, ma è più semplice.

A settembre usciranno importanti novità, per cui chi aspetta compra meglio, però rinvia i benefici. Per chi deve avere con sé tanti documenti per lavoro (per esempio manuali tecnici) e per chi legge tanto, magari in viaggio, specialmente se sa l'inglese, già ora i benefici sono grandi e i prezzi sono abbordabili.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 6.11

Doppioclick: nuovi suffissi Internet, vantaggi e rischi

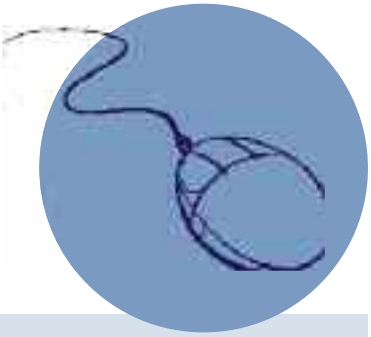
Tra pochi mesi un indirizzo Internet come "consigli.borsadellaspesa", senza il consueto ".com" o ".ch" finale, non sarà più un errore. A gennaio 2012, infatti, si aprirà la prenotazione dei cosiddetti "nomi di dominio generici di primo livello", che entrerà in funzione entro la fine dello stesso anno: tradotto in italiano, vuol dire che la parte finale del nome di un sito Internet non sarà più limitata ai vari ".com", ".gov", ".org" e alle sigle degli stati (per esempio ".fi", ".fr", ".de") ma potrà essere qualunque sequenza di simboli in qualunque alfabeto.

È una rivoluzione delle regole di Internet decisa dall'ICANN, l'ente che gestisce questi nomi di dominio di primo livello. Lo scopo di questo cambiamento è consentire alle aziende e a chi detiene un marchio importante di avere una presenza su Internet facilmente memorizzabile. Oggi, per esempio, è facile dimenticarsi se un sito è un ".com" o un ".org"; invece domani un'azienda che acquisterà uno di questi nuovi suffissi potrà essere raggiunta su Internet semplicemente digitandone il nome. Il privilegio, però, costerà caro: 185.000 dollari per ogni nome richiesto. Inoltre sarà necessario dimostrare di essere titolari del marchio registrato corrispondente.

Per gli utenti questa novità comporta alcune cautele. Sarà necessario aggiornare i programmi di navigazione e i sistemi operativi, perché quelli attuali potrebbero non riconoscere i nuovi nomi. Inoltre i truffatori della Rete approfitteranno del cambiamento e della conseguente confusione per creare nuove trappole attraverso nomi ingannevoli o ambigui: **.borsadeIIaspesa** è diverso da **.borsadellaspesa**, ma quanti se ne accorgeranno?

Visti i costi, comunque, è anche possibile che siano poche le adesioni a questi nuovi nomi e che tutto si concluda con un nulla di fatto. Non sarebbe la prima volta: quanti siti .museum o .aero conoscete? Eppure questi due suffissi sono attivi dal 2000 insieme a .biz, .coop, .info, .name e .pro. Almeno per i primi mesi, comunque, sarà prudente non fidarsi ciecamente degli inviti a visitare siti i cui nomi sono privi delle classiche sigle finali precedute dal punto.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 7.11

Doppioclick: Bitcoin, i soldi virtuali e anonimi di Internet

Pagare via Internet è spesso un problema: molti non si fidano a usare la carta di credito e non vogliono fare acquisti tracciabili, per esempio per non far sapere al partner quanto hanno speso per il suo regalo. Una soluzione per i pagamenti anonimi online è Bitcoin (www.bitcoin.org), una "moneta virtuale" creata nel 2009.

È una moneta decisamente atipica: è immateriale, non si sa chi sia il suo creatore (si fa chiamare Satoshi Nakamoto, ma la sua identità reale è sconosciuta), non ha una banca centrale e consente acquisti anonimi ma al tempo stesso trasparenti: ogni transazione di Bitcoin è pubblicamente consultabile da chiunque, senza però rivelare le identità dei partecipanti. Non ci sono intermediari o commissioni, esattamente come per il contante tradizionale. Non sorprende, quindi, che sia uno dei mezzi di pagamento utilizzati dalla criminalità informatica e da chi vuole eludere i blocchi nazionali sui siti di scommesse ma anche da chi vive in paesi soggetti a censura ma vuole acquistare online, per esempio, un libro bandito nel suo paese.

La quantità di Bitcoin è fissa e immutabile, non è possibile creare soldi virtuali falsi e tutti i movimenti di denaro avvengono senza un sito centrale di coordinamento. Procurarsi dei Bitcoin è facile: basta rivolgersi a uno dei vari siti che fungono da agenzie di cambio e permettono di acquistare Bitcoin in cambio di valute tradizionali oppure mettere in vendita un oggetto o un servizio e accettare pagamenti in Bitcoin.

Sembra un sistema perfetto, ma esattamente come il denaro contante, anche i Bitcoin possono essere rubati. Il "portafogli" digitale nel quale ciascun utente custodisce i propri Bitcoin è un file, di nome wallet.dat, che risiede nel suo computer. Se qualcuno riesce ad impossessarsene (per esempio usando virus come Infostealer.Coinbit, già in circolazione), può spenderne anonimamente il contenuto. Sono già stati segnalati furti per decine di migliaia di franchi.

Inoltre il sistema di gestione di Bitcoin ha falle che possono causare svalutazioni improvvise: a giugno di quest'anno uno dei suoi siti di cambio, Mt. Gox, è stato colpito da un'intrusione che ha aperto la strada a una svendita in massa di Bitcoin, il cui valore è precipitato di colpo quasi a zero, consentendo agli intrusi di effettuare speculazioni da riconvertire subito in denaro tradizionale. Il tentativo è fallito, ma ha dimostrato che per ora è opportuno non affidare grandi somme a questa moneta digitale.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 8.11

Doppioclick: MELANI spiega i rischi per gli internauti svizzeri

MELANI è l'acronimo della Melde- und Analysestelle Informationssicherung o Centrale d'annuncio e d'analisi per la sicurezza dell'informazione dell'Amministrazione Federale, che ha il compito di proteggere le infrastrutture critiche del nostro Paese (energia, banche, telecomunicazioni), in particolare quelle legate alle tecnologie d'informazione e comunicazione.

Periodicamente MELANI pubblica, presso http://www.melani.admin.ch, un rapporto che fa il quadro dei rischi informatici che possono colpire gli utenti Internet in Svizzera: è una lettura molto interessante, anche se un po' tecnica, che rivela lo stacco fra rischi percepiti dall'opinione pubblica e rischi reali.

Per esempio, molti utenti temono attacchi informatici ai propri conti correnti bancari, ma in realtà le protezioni elevate di questo settore hanno spostato l'attenzione dei criminali verso altri servizi online, meno protetti, attraverso i quali gli utenti muovono denaro o beni equivalenti, come eBay, PayPal e giochi in rete. Il vero pericolo per i conti bancari è indiretto: passa attraverso la sottrazione dei dati delle carte di credito e affini, che secondo MELANI in Svizzera ha subìto un aumento imponente (225 casi contro i 135 del 2010) tramite la tecnica dello "skimming", ossia la lettura abusiva dei dati e dei codici delle tessere attraverso dispositivi nascosti, applicati a bancomat e altri apparecchi di pagamento. Bisogna sempre coprire la mano mentre si digita il PIN ed esaminare con attenzione ogni dispositivo nel quale si inserisce la tessera. Le banche, comunque, solitamente compensano il cliente derubato se è chiaro che non ha commesso negligenza grave.

La forma d'intrusione principale su Internet è invece il "drive-by", nel quale è sufficiente visitare una pagina infetta di un sito per trovarsi il computer sotto attacco. Queste pagine sono spesso ospitate inconsapevolmente da siti innocenti e rispettabili che sono stati violati e l'utente viene attirato su di esse quando effettua ricerche in Google. MELANI ha bloccato numerosi casi di "drive-by" riguardanti siti svizzeri; l'utente può tutelarsi usando programmi di navigazione aggiornati e prudenza nel condurre ricerche su argomenti controversi o d'attualità.

La segnalazione più bizzarra della Centrale riguarda le infezioni informatiche volontarie: le cercano soprattutto gli utenti di iPhone, iPad e iPod di Apple, che tolgono le protezioni del proprio dispositivo per potervi installare applicazioni senza passare dal servizio ufficiale iTunes. La tecnica si chiama "jailbreak" ed è diffusissima fra i giovani, ma è l'equivalente di togliersi la cintura di sicurezza perché dà fastidio.

PAOLO ATTIVISSIMO