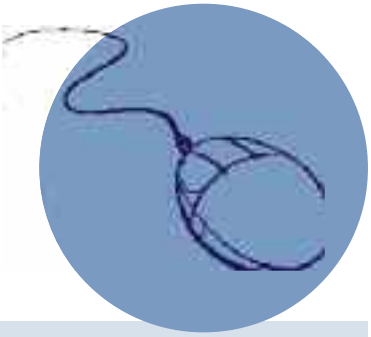


La Borsa *della* Spesa
Edizione 1.12

Doppioclick: chi fabbrica le catene di Sant'Antonio?

Appelli per bambini malati di leucemia in cerca di donatori di sangue, allarmi per virus informatici letali, promesse di guadagni facili grazie a Bill Gates e altro ancora: gli argomenti delle catene di Sant'Antonio che girano su Internet e in particolare su Facebook sono tanti e molto eterogenei, ma sono tutti accomunati dalla richiesta perentoria di inoltrarli il più possibile. Questo li ha trasformati in una delle piaghe di Internet e molti utenti si chiedono chi abbia così tanto interesse a generare e diffondere queste catene e se possano esserci dei danni.

È raro che queste catene siano fabbricate da chi vuole disseminare virus informatici, per cui non costituiscono un pericolo tecnico diretto. Talvolta vengono confezionate dagli spammer, i pubblicitari-spazzatura di Internet, per collaudare i propri sistemi di distribuzione delle pubblicità indesiderate, ma di solito nascono in buona fede: un utente viene a conoscenza di una notizia o ne è protagonista diretto (per esempio i genitori di un bambino malato) e la diffonde agli amici, i quali la inoltrano ai loro amici, e così via. Spesso la notizia è un equivoco o viene distorta dal passaparola, ma la buona fede iniziale rimane. In casi come questi il danno è involontario ma è reale, perché in queste catene confluiscono centinaia di indirizzi di e-mail di destinatari, che vengono poi raccolti dagli spammer per inondarci di mail pubblicitarie indesiderate, causando scocciature e perdite di tempo. Se proprio si vuole inoltrare una catena di Sant'Antonio, quindi, sarebbe opportuno farlo nascondendo l'elenco dei destinatari: tutti i principali programmi di gestione della mail lo consentono (funzione "BCC" o "CCN" o "copia carbone nascosta").

In alcuni casi, molto rari, si riesce a risalire al creatore di una catena. È successo, per esempio, con quella che promette un compenso in denaro, offerto da Microsoft, per chiunque inoltri la catena a un certo numero di contatti: la catena sarebbe infatti un test di Internet Explorer. Non è vero: si tratta di una burla inventata nel 1997 da Bryan Mack, all'epoca studente nell'Iowa, per parodiare le offerte per fare soldi in fretta via Internet che spopolavano già allora. Mack la inviò per scherzo ai propri amici, che la diffusero a macchia d'olio. Alcuni la presero sul serio e da lì nacque il mito. Prudenza, quindi, prima di inoltrare; se non c'è modo di verificare una catena, è meglio non diffonderla.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 2.12

Doppioclick: miniguida a Twitter, il micro-social network del momento

Centoquaranta caratteri, non uno di più: questo è il limite di lunghezza di ogni messaggio di Twitter (www.twitter.com), social network emergente, alternativo o complementare al popolarissimo Facebook e usatissimo per la diffusione fulminea di notizie.

Un limite che colpisce e intriga subito perché è una sfida linguistica e un invito alla concisione: l'esatto contrario delle chiacchiere prolisse degli altri social network.

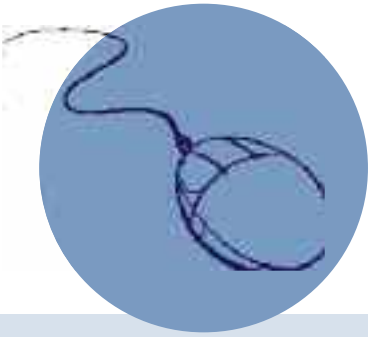
Iscriversi è facile e gratuito: scegliete un nome o pseudonimo (meglio se breve) e da quel momento siete identificati su Twitter da quel nome preceduto dalla chiocciolina. Poi selezionate gli amici o i servizi dai quali volete ricevere aggiornamenti (per esempio @RSIonline per la Radiotelevisione Svizzera) e cliccate su Segui. Inizierete a ricevere un flusso di aggiornamenti nel vostro profilo Twitter o attraverso le applicazioni apposite per iPad, iPhone e telefonini Android.

Quando avete qualcosa da dire, digitatelo nella casella Scrivi un nuovo tweet (si chiamano così i messaggi di Twitter). Potete anche mandare un tweet tramite SMS a un apposito numero (estero, quindi occhio ai costi): utile se siete in roaming o avete un telefonino che non va su Internet. Tenete presente che su Twitter tutti i messaggi sono pubblici e visibili a chiunque salvo diversa impostazione. Inoltre è possibile integrare Twitter con Facebook in modo che ogni vostro tweet appaia anche nel vostro profilo Facebook.

Se quello che scrivete piace, altri utenti inizieranno a seguirvi e a diffondere o commentare i vostri tweet (questo si chiama retweetare). Potete includere un link (un indirizzo di un sito, per esempio) in un tweet: verrà abbreviato automaticamente. Ai messaggi si possono anche allegare foto, cliccando sull'icona Aggiungi un'immagine, e i dati di geolocalizzazione (l'indicazione di dove ci si trova in quel momento; attenzione, in questo caso, alla privacy). Se iniziate un messaggio con il nome di un utente, Twitter lo considererà una risposta rivolta a quell'utente, e se seguite un utente e lui segue voi potete scambiare messaggi privati. Ci sono anche delle parole chiave, chiamate hashtag, che iniziano con il simbolo "#" e servono per raggruppare messaggi dedicati a un tema (per esempio #sapevatelo oppure #terremoto).

Sostituirà Facebook? Improbabile. Ma per chi vuole restare aggiornato sugli eventi senza distrazioni pubblicitarie, Twitter in questo momento è impagabile.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 3.12

Doppioclick: diario di Facebook, rischio d'imbarazzo

Da alcuni mesi Facebook sta introducendo il Diario (Timeline in originale): l'organizzazione dei contenuti secondo una linea temporale, situata al centro della pagina.

In primo piano ci sono gli elementi appena pubblicati, seguiti da quelli via via meno recenti, disposti alternati ai lati della linea; in alto a destra c'è un indice suddiviso in mesi e anni. Lo scopo del Diario è spingerci a condividere sempre più informazioni personali, che sono la fonte primaria di guadagno di Facebook: non solo gli eventi successivi alla nascita del social network, ma anche tutta la storia della nostra vita.

Questa nuova struttura comporta dei rischi non intuitivi, perché l'indice cronologico rende molto più facile a chiunque accedere a quello che abbiamo pubblicato mesi o anni prima. Magari nel frattempo abbiamo cambiato lavoro, partner, affiliazione politica o gusti musicali o di abbigliamento, ma le nostre vecchie opinioni e fotografie sono ancora lì, fresche come quando le abbiamo pubblicate, anche se non ci rispecchiano più. Per esempio, per il nostro nuovo partner può essere motivo di disagio vederci in foto in compagnia dell'ex amore e per chiunque è più facile farsi i fatti nostri sfogliando quello che a questo punto è un vero e proprio diario pubblico.

È molto più facile trovare vecchi contenuti e diffonderli, tolti dal contesto temporale, per causarci imbarazzi.

Per contenere questo rischio bisognerebbe sfogliare, valutare e regolare le impostazioni di privacy di ogni cosa che abbiamo pubblicato, ma c'è una scorciatoia: nelle Impostazioni sulla privacy c'è la voce Restringi il pubblico per i vecchi post, che consente di modificare in blocco la visibilità di tutti i vecchi elementi pubblicati, rendendoli tutti accessibili soltanto agli amici anche se prima erano visibili a tutti o agli amici degli amici.

Questa modifica globale va valutata con attenzione, perché è reversibile soltanto modificando manualmente la privacy di ciascun elemento e non offre un oscuramento totale. Per togliere completamente dal Diario un elemento bisogna visualizzarlo, posizionarvi sopra il cursore in modo da far comparire una casella con una matita, sulla quale si clicca per far comparire un menu dal quale si sceglie.

Nascondi dal diario (c'è anche l'opzione Elimina post per eliminare l'elemento). In alternativa si può cliccare sull'icona di privacy dell'elemento, accanto alla sua data di pubblicazione, per cambiarne le impostazioni di privacy.

Paolo Attivissimo

La Borsa *della* Spesa
Edizione 4.12

Doppioclick: attenzione alla truffa dell'amico all'estero

Ricevete da un amico una mail angosciante: l'amico è all'estero ed è stato aggredito e derubato di tutto: telefonino, carta di credito, contanti, documenti. Per tornare in patria gli serve urgentemente del denaro, da inviare tramite Western Union o un altro sistema di pagamento rapido internazionale.

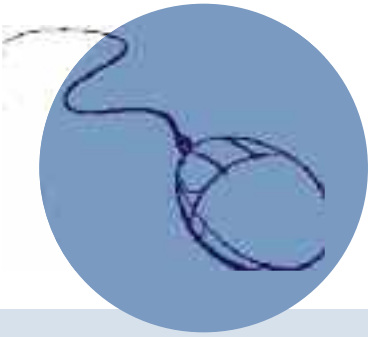
A sangue freddo una descrizione del genere suscita subito il sospetto di una truffa, ma quando capita di ricevere veramente un messaggio di questo genere è sorprendentemente facile cadere nella trappola. L'emozione ci fa mettere in disparte la razionalità e ci impedisce di notare che spesso la mail-trappola è stranamente sgrammaticata e di chiederci se la situazione è plausibile e di fare il controllo più semplice: il nostro amico è davvero all'estero? Magari basta una telefonata per scoprirlo. Ma in una situazione drammatica il dubbio non nasce.

La truffa è convincente anche per un altro motivo: proviene dall'indirizzo di mail dell'amico. O almeno così pare, ma molti non sanno che in realtà l'indirizzo del mittente di una mail è facilmente falsificabile in vari modi. Il più semplice è usare un indirizzo molto simile (per esempio luigi.rezzonico@ticino.ch al posto di luigi.rezzorico@ticino.ch), ma capita anche che il truffatore prenda il controllo della vera casella di mail del nostro amico dopo avergli rubato la password.

Quello che maggiormente impedisce a molte vittime di pensare alla truffa, però, è un dubbio: come fa un truffatore a sapere che l'amico e la vittima si conoscono? In realtà il legame di conoscenza o amicizia è facile da scoprire per un criminale. Se il truffatore ha preso possesso della casella di mail dell'amico, ha accesso alla sua rubrica degli indirizzi e quindi la usa per mandare la stessa esca a tutti gli indirizzi presenti nella rubrica. Se ha preso il controllo del profilo Facebook dell'amico, può guardare gli indirizzi dei suoi amici su Facebook. A volte non occorre neanche impossessarsi del profilo Facebook, perché molti utenti lasciano che il proprio indirizzo di mail e le proprie amicizie siano visibili a chiunque. Raccogliere i dati per la truffa, in questo caso, è semplicissimo.

Difendersi, però, è altrettanto semplice: già sapere dell'esistenza e del meccanismo di questa truffa è un buon vaccino. Per maggiore scrupolo conviene nascondere il proprio indirizzo di mail in Facebook, nelle informazioni di contatto, applicandovi "Solo io" come livello di privacy.

Paolo Attivissimo



La Borsa *della* Spesa
Edizione 5.12

Doppioclick: Computer bloccato dalla SUISA? Telefonate da Microsoft? Occhio alle truffe

Se vi compare di colpo sul computer un avviso con il logo del Dipartimento di Giustizia e Polizia o della SUISA che vi informa che il PC è bloccato perché sono state rilevate attività illegali e c'è una multa da pagare per lo sblocco, non vi spaventate: si tratta in realtà di truffe organizzate da criminali che si spacciano per le autorità, infettano i computer con virus che visualizzano questi avvisi e stanno mietendo moltissime vittime anche in Svizzera. Se pagate, i soldi vanno ai truffatori, insieme ai codici della vostra carta di credito.

Per sbloccare il computer occorre riavviarlo usando un antivirus su CD o su penna USB capace di scavalcare Windows. Se non ne avete uno, chiedete a un collega di scaricarlo da Internet per voi oppure provate questo trucco: premete il tasto F8 durante il riavvio, in modo da arrivare a una schermata di testo che parla di "modalità protetta con prompt dei comandi". Poi digitate "explorer": parte Esplora Risorse, con il quale andate a C:\windows\system32\restore\ (se usate Windows XP) oppure C:\windows\system32 (se usate Windows Vista/7) e avviate il programma rstrui.exe, che riporta il computer a un punto di ripristino precedente l'infezione. Per evitare la reinfezione in futuro, aggiornate il vostro antivirus e usatelo su tutto quello che scaricate, specialmente le applicazioni e i giochi.

Se invece ricevete una telefonata (spesso in inglese) da persone che dicono di essere del servizio clienti Microsoft, affermano di aver rilevato un virus nel vostro computer e si offrono di aiutarvi a rimuoverlo, non abboccate e non seguite le loro istruzioni, ma riappendete: è un'altra forma di truffa particolarmente sfacciata che sta circolando da alcuni mesi. Le istruzioni che vi danno fanno effettivamente comparire sullo schermo messaggi dall'aria preoccupante, ma si tratta di un inganno: in realtà sono normali messaggi di test di Windows.

Lo scopo dei truffatori, in questo caso, è prendere il controllo del vostro computer ed estorcervi del denaro dicendo che dovete pagare per rimuovere il virus (che in realtà non esiste). Purtroppo le denunce alla Polizia possono fare poco, perché i criminali stanno quasi sempre all'estero, e quindi dobbiamo essere noi la nostra prima linea di difesa.

Paolo Attivissimo

La Borsa *della* Spesa
Edizione 6.12

Doppioclick: antifurto per Facebook

Per contrastare il problema dei furti di account Google/Gmail e Facebook c'è da poco una nuova protezione che ha un nome complicato ma è facile da usare ed è altamente consigliabile: un SMS che vi segnala e blocca qualunque tentativo di accedere al vostro account da un computer, tablet o smartphone che non sia il vostro.

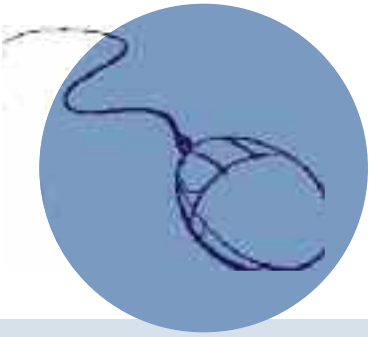
Il sistema si chiama formalmente "autenticazione a due fattori": vuol dire che per accedere a un account non basta conoscerne la password ma bisogna anche conoscere un codice supplementare che arriva con un SMS gratuito. Facebook la chiama "Notifica di accesso" e la colloca nelle Impostazioni Account, sotto la voce Protezione - Notifiche di accesso e Approvazione degli accessi. Google, invece, la definisce "Verifica in due passaggi" e la offre sotto Impostazioni Account - Sicurezza.

In entrambi i casi bisogna affidare a questi servizi un proprio numero di telefono cellulare, che non viene reso pubblico e che non comporta seri rischi per la privacy (considerato che Google e Facebook hanno già accesso a tutte le mail, le foto e gli altri dati che vi avete caricato).

Fatto questo, ogni volta che accederete al vostro account Facebook o Google/Gmail riceverete un SMS con un codice di autenticazione da immettere in aggiunta alla password. Dato che il codice arriva soltanto a voi, l'eventuale intruso che vi abbia rubato la password non potrà entrare.

Per evitare che vi venga chiesto questo codice supplementare ogni volta che accedete usando il vostro cellulare o computer, potete definire un elenco di dispositivi fidati. In questo modo la protezione offerta dall'autenticazione a due fattori sarà trasparente per voi ma molto difficile da scavalcare per gli intrusi, che dovrebbero avere accesso fisico al vostro dispositivo per poter agire contro quest'antifurto: un'eventualità molto improbabile, dato che solitamente i tentativi d'intrusione vengono effettuati da lontano via Internet, pescando a casaccio.

Paolo Attivissimo



La Borsa *della* Spesa
Edizione 7.12

Doppioclick: arriva Windows 8, che fare?

Se state pensando di cambiare computer e avete notato il recente debutto di Windows 8, la nuova versione del sistema operativo di Microsoft, probabilmente vi state chiedendo se inseguire questa novità oppure restare fedeli alle versioni precedenti. Non è un dubbio da poco, perché Windows 8 è radicalmente differente dalle edizioni passate, in particolare a livello visivo: sparisce il menu Start, punto di partenza ormai consueto da quasi vent'anni, e al suo posto c'è una schermata suddivisa in "piastrelle" personalizzabili e interattive. All'inizio è disorientante, ma ci si abitua presto, soprattutto se il computer ha uno schermo tattile, perché Windows 8 è pensato proprio per essere usato toccando lo schermo con le dita, anche se resta usabile con il mouse o touchpad tradizionale.

Inoltre il nuovo aspetto esteriore di Windows 8 è quasi identico a quello dei telefonini Windows Phone, per cui ci si trova con lo stesso modo di comandare entrambi i dispositivi invece di doverne imparare due differenti. Anche i tablet di Microsoft, denominati Surface e caratterizzati dalla disponibilità di una tastiera nella copertura dello schermo, usano Windows 8, unificando ulteriormente l'uso di tutti i dispositivi più di quanto faccia la concorrenza di Apple.

Un'altra semplificazione è l'installazione centralizzata delle applicazioni tramite il sito Windows Store, come già fa Apple con l'App Store.

Attenzione, però: i tablet Surface di base (quelli con processore ARM) potranno installare soltanto le applicazioni disponibili tramite Windows Store, mentre gli altri Surface saranno liberi d'installare qualunque applicazione, come un computer tradizionale.

Dietro le quinte ci sono anche notevoli miglioramenti in fatto di sicurezza e riduzione dei consumi, ma comunque non c'è fretta di migrare: Microsoft garantirà il supporto tecnico primario per Windows 7 fino a gennaio 2015. Inoltre i prezzi dei prodotti informatici calano in continuazione, per cui conviene aspettare il più a lungo possibile per ottenere il massimo risultato con la minima spesa.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 8.12

Doppioclick: telefonini riciclati attenzione ai dati personali

Capita spesso di passare a un modello nuovo di telefono cellulare e regalare, vendere o dare in beneficenza quello vecchio, ma capita meno spesso di pensare a cosa succede alle informazioni personali custodite nel telefono dismesso: foto, rubriche con numeri e nomi confidenziali, registri delle telefonate fatte e ricevute, messaggi, password di servizi e altro ancora. Se non vengono cancellati, saranno a disposizione di chi riceverà il telefono.

Le organizzazioni benefiche serie e gli operatori telefonici si rivolgono a servizi appositi di cancellazione di questi dati (il cosiddetto "wiping"), che danno buone garanzie ma restano pur sempre luoghi nei quali un addetto malintenzionato potrebbe fare raccolta di dati su vasta scala.

È quindi consigliabile in ogni caso cancellare personalmente i dati prima di cedere il telefonino. Per prima cosa occorre rimuovere la SIM, anche se è stata disattivata dall'operatore, perché contiene numerosi dati personali facilmente leggibili. Poi bisogna togliere eventuali schede di memoria rimovibili (Micro SD e simili), anche perché probabilmente si potranno riusare nel nuovo telefonino. Fatto questo, ogni cellulare ha una funzione apposita di "hard reset" (azzeramento) che lo ripristina alle condizioni di fabbrica e va usata invece della semplice cancellazione manuale dei dati, che lascia comunque tracce recuperabili con appositi programmi.

Trovare la funzione di azzeramento per il modello specifico non è sempre facile: di solito è indicata nel manuale (se l'avete smarrito, ne potete scaricare una copia dal sito del fabbricante), ma se non c'è ci si può rivolgere ai siti degli operatori di telefonia mobile o a quelli degli appassionati. Una ricerca in Google con il nome del vostro telefonino e le parole "erase" o "hard reset" porterà facilmente a video esplicativi.

PAOLO ATTIVISSIMO