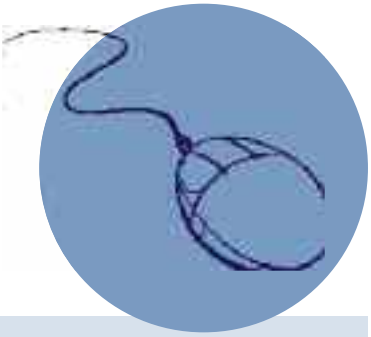


La Borsa *della* Spesa
Edizione 1.13

Doppioclick: televisori "intelligenti" Attenti a collegarli a internet

I televisori di oggi sono in realtà dei veri e propri computer mascherati da TV. Sono spesso collegabili a Internet tramite cavo o WiFi per poter navigare nel Web e seguire i canali TV della Rete, hanno porte USB alle quali collegare dischi rigidi esterni e schede di memoria di fotocamere e i modelli di punta di molte marche obbediscono alla voce o ai gesti. Funzioni quasi fantascientifiche, ma con implicazioni di sicurezza che non sempre sono state considerate a fondo.

La connessione a Internet, infatti, espone al pericolo di intrusioni informatiche. Non è un rischio teorico: i ricercatori di ReVuln, azienda specializzata in sicurezza informatica, sono riusciti a prendere il controllo via Internet di una Smart TV Samsung, leggendo i dati personali (foto, video e documenti), alterando la configurazione del telecomando, cambiando i canali a distanza e installando nel televisore del software ostile.

L'idea che un intruso digitale possa sapere quali programmi guardiamo e sfogliare le nostre foto personali può dare fastidio, ma non più di tanto, e comunque sembra un movente misero per un crimine informatico reale. Le cose cambiano se il televisore "intelligente" è dotato di comandi vocali o gestuali, perché queste funzioni implicano la presenza di microfoni e telecamere nell'apparecchio: diventa quindi possibile spiare e origliare nelle case o negli uffici nei quali si trovano questi televisori. È già successo con le telecamere della Trendnet, come si può vedere presso http://cams.hhba.info.

Samsung distribuirà a breve una correzione per questa falla: il problema sarà informare chi ha acquistato questi apparecchi, perché a differenza dei computer questi televisori non hanno un sistema di aggiornamento automatico e quindi potrebbero restare non aggiornati e vulnerabili a lungo. In attesa della correzione, all'utente conviene controllare le protezioni del proprio punto di accesso a Internet e valutare se scollegare il televisore dalla Rete. O magari acquistare televisori meno intelligenti.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 2.13

Doppioclick: perché i computer della Apple sembrano immuni ai virus?

Uno dei miti più diffusi dell'informatica è l'apparente invulnerabilità dei computer della Apple ai virus. In realtà anche questi computer sono infettabili con relativa facilità (non con virus veri e propri ma con altri tipi di "malware", come i "cavalli di Troia" o "Trojan horse"), ma i criminali informatici preferiscono pescare dove ci sono più pesci e quindi si dedicano al bersaglio numericamente più ampio, costituito dai computer che usano le varie versioni di Windows (circa il 90% di tutti i computer fissi). Così creano principalmente virus per Windows, che non funzionano sui computer della Apple. In sostanza, i Mac sembrano invulnerabili anche perché vengono presi molto meno di mira.

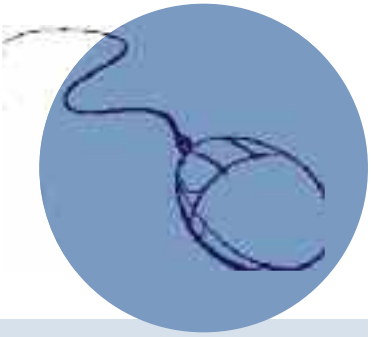
Questo stato di cose, però, sta cambiando, tanto che dal 2009 Apple ha silenziosamente aggiunto ai propri computer una sorta di "antivirus" integrato, chiamato Xprotect/File Quarantine, e ci sono stati attacchi, come quello denominato Flashback, che hanno infettato fino a 600.000 computer Apple nel mondo.

La chiave di questo sgradevole cambiamento si chiama Java, un software che permette di scrivere programmi che funzionano sia su computer Apple, sia su computer Windows e consente quindi ai criminali di creare "virus" che possono infettare anche i Mac praticamente senza nessuna fatica aggiuntiva.

Difendersi è comunque facile: sui Mac basta controllare con un buon antivirus aggiornato tutto quello che si riceve, disinstallare o disattivare Java, che di solito non serve (in Safari, si va in Preferenze > Sicurezza e si toglie la spunta ad "Abilita Java"; in Firefox, si va in Strumenti > Componenti aggiuntivi > Plugins e si disabilita tutto quello che riguarda Java), e non installare programmi di provenienza dubbia, che possono essere cavalli di Troia: se il Mac si rifiuta di installarli, probabilmente si è accorto che sono stati alterati e non conviene forzare l'installazione.

Per iPad, iPod e iPhone, invece, l'antivirus non serve se l'utente non li "cracca", cioè ne toglie le protezioni fornite dal fabbricante, per installare programmi non approvati da Apple.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 3.13

Doppioclick: riciclare i computer? Sì, ma attenzione alla sicurezza

Ben 60.000 tonnellate di rifiuti elettronici sono state riciclate in Svizzera nel 2012: ma quanti PC, in quelle tonnellate, sono stati mandati al riciclaggio senza prima rimuoverne i dati personali e le password?

Recuperare dati da un PC "rottamato" è banalissimo: basta estrarne il disco rigido e inserirlo in un altro computer, usando eventualmente gli appositi software di analisi e recupero dati. Emergono foto personali, dati contabili e medici, password, mail, cronologia dei siti visitati, musica, film e programmi commerciali recuperabili in violazione delle licenze e del diritto d'autore.

Il rischio riguarda tutta la filiera del riciclaggio: anche se le norme e i controlli sono severi, la possibilità che qualche mela marcia approfitti della situazione rimane. Ne sa qualcosa il cantante Paul McCartney, i cui dati contabili furono trovati su un computer dismesso da una banca britannica. Anche le fotocopiatrici professionali sono a rischio: molte contengono un disco rigido sul quale rimane una copia digitale dei documenti fotocopiati.

Questi dati devono insomma essere distrutti in qualche modo. La cancellazione semplice del disco non è sufficiente, perché i programmi di recupero (usati anche dalle forze di polizia) sono in grado di ripristinare quasi tutti i dati eliminati. Anche la formattazione standard non basta: servono programmi di cosiddetto "wiping" professionale, che riscrivono l'intero disco più volte. Ma questa procedura può richiedere ore.

Se il computer è da buttare e non verrà riutilizzato, c'è un metodo drastico ma efficacissimo e veloce, ed è quello usato dai professionisti del settore: distruggere fisicamente il disco rigido usando un trapano per trapassarlo. Questo riduce in mille pezzi le fragili parti interne, che restano però racchiuse nel guscio esterno, in modo ordinato, compatto ed ecologico. Se poi si tratta di un computer che vi ha fatto tribolare, c'è la gratificazione non trascurabile di sfogarsi fisicamente a colpi di trapano.

Paolo Attivissimo

La Borsa *della* Spesa
Edizione 4.13

Doppioclick: antivirus anche sui telefonini?

I telefonini, specialmente i cosiddetti "smartphone", sono sempre più simili a computer: viene spontaneo chiedersi se siano altrettanto infettabili dai virus informatici e se abbia senso dotarli di un antivirus.

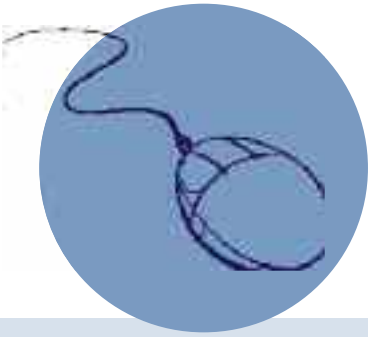
In effetti esistono "virus" (più propriamente "malware") sia per i cellulari evoluti, sia per quelli semplici, e tutti i telefonini sono un bersaglio particolarmente goloso per i criminali informatici, non solo per la quantità d'informazioni personali che contengono (foto, indirizzi, numeri di telefono, mail), ma anche perché danno accesso diretto al portafogli del proprietario, per esempio con i malware che mandano SMS a tariffa maggiorata a operatori telefonici esteri compiacenti.

Per ridurre il rischio di farsi infettare ci sono alcune regole preliminari importanti: non installare applicazioni provenienti da fonti differenti da quelle regolari (App Store, Google Play, Windows Phone Store), neanche se le invia una persona fidata (che può essere stata ingannata o infettata a sua volta); non "craccare" gli iPhone (togliendo le loro protezioni) per installarvi app piratate; non accettare, o aprire con cautela, i file inviati tramite Bluetooth o come allegati a una mail; e tenere libero da infezioni l'eventuale computer al quale si collega lo smartphone per la sincronizzazione.

È prudente accompagnare questi comportamenti con un buon antivirus (gratuito o a pagamento) sul telefonino: Avast, Intego, Kaspersky, Lookout, McAfee, Norton, Sophos, Trend Micro, TrustGo sono alcuni dei nomi più qualificati in questo campo e offrono anche funzioni di tracciamento o di blocco in caso di furto o smarrimento. Occorre scaricare questi prodotti direttamente dai siti dei rispettivi produttori, per evitare di incappare in falsi antivirus.

Non va dimenticato, infine, che quello che non c'è non si può rompere, per cui è meglio scegliere telefoni cellulari che non abbiano troppe funzioni che non ci servono e non installare app che non siano realmente necessarie. La semplicità è spesso la miglior forma di sicurezza.

Paolo Attivissimo



La Borsa *della* Spesa
Edizione 5.13

Doppioclick: WhatsApp e Ruzzle, rischi per sicurezza e privacy

Ci sono molte app popolarissime, come WhatsApp e Ruzzle, che permettono di scambiare messaggi o di giocare in gruppo tramite il telefonino, il tablet o il computer; usarle può offrire risparmi consistenti sulla bolletta. Ma occorre fare attenzione, perché queste app, gratuite o quasi, spesso si pagano attraverso la cessione di dati personali e una riduzione della sicurezza.

Per esempio, quasi tutte le versioni di WhatsApp obbligano l'utente a trasmettere all'azienda produttrice dell'app tutti i numeri di telefono contenuti nella propria rubrica, compresi quelli del proprio avvocato o medico o dei propri contatti riservati di lavoro e persino quelli di chi non è iscritto a WhatsApp e non lo vuole usare. Per questa pesca a strascico indiscriminata di dati, WhatsApp è già finito nei guai con le autorità di tutela della privacy in Canada e nei Paesi Bassi.

Nel caso di Ruzzle, invece, è emersa recentemente una falla di sicurezza che permetteva di assumere l'identità di un utente qualsiasi e leggere i suoi messaggi privati, e un problema analogo ha colpito WhatsApp, con tutte le implicazioni per truffe, equivoci, imbarazzi e furti d'identità che ne derivano. Queste vulnerabilità sono state in parte risolte, ma resta il dubbio che molte app siano realizzate con poca attenzione a privacy e sicurezza (le falle erano davvero dilettantesche) e molta al profitto: i dati personali vengono spesso rivenduti a fini pubblicitari o di sorveglianza.

Conviene quindi valutare attentamente se il risparmio offerto da queste app giustifichi il rischio concreto di trovarsi spiati o truffati o di svendere dati personali o professionali riservati, propri e altrui, e in particolare è prudente evitare di installarle su dispositivi usati per lavoro. Anche in informatica, le cose gratuite sono spesso quelle che possono costare di più.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 6.13

Doppioclick: Siamo tutti spiati Cosa può cambiare per l'utente comune

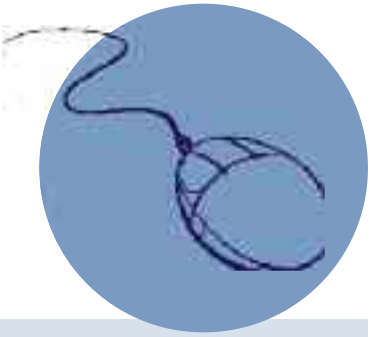
Le rivelazioni dell'informatico Edward Snowden ci pongono tutti di fronte a un fatto non più eludibile: le comunicazioni via Internet effettuate tramite i grandi fornitori di servizi (Google, Apple, Microsoft, Yahoo e altri) vengono intercettate su vastissima scala dall'NSA (National Security Agency) statunitense e da altri servizi di intelligence di vari governi del mondo. Se avete mai inviato o ricevuto una mail tramite Gmail, per esempio, è presumibile che una sua copia sia archiviata negli immensi depositi dell'NSA.

Viene istintivo pensare che questo sia un problema soltanto per terroristi, criminali e agenti segreti ma in realtà tocca molti di noi che per lavoro si trovano a gestire dati sensibili: giornalisti, medici, avvocati, operatori di borsa, imprenditori, dipendenti di banche, compagnie assicurative, ospedali e amministrazioni pubbliche. Tutte queste figure hanno vincoli (spesso codificati dalla legge) sulla riservatezza dei dati, che non possono garantire se usano il cosiddetto "cloud" con fornitori statunitensi.

Una ginecologa che invia referti medici alla paziente attiva in campo politico, una banca che recapita gli estratti conto dei clienti su una casella Gmail o custodisce documenti contabili su Google Docs, Microsoft SkyDrive o Dropbox (succede), o un'azienda che deposita nel "cloud" i piani commerciali o i progetti di nuovi prodotti, non può più fingere di ignorare che li rende leggibili a uno o più governi stranieri, che li usano per il proprio tornaconto.

Le implicazioni legali e commerciali sono profonde ma spesso ignorate perché comportano cambiamenti onerosi. Si stima che l'"effetto Snowden" farà perdere alle aziende "cloud" americane contratti esteri per 35 miliardi di dollari: soldi che si potranno riversare anche nell'industria svizzera della conservazione sicura dei dati, che per questo sta già costruendo bunker digitali a prova di NSA che beneficiano dell'immagine di neutralità e riservatezza della Svizzera. Meglio pensarci.

PAOLO ATTIVISSIMO



La Borsa *della* Spesa
Edizione 7.13

Doppioclick: WeChat e SnapChat trappole per la privacy

WeChat e SnapChat, due "app" popolarissime soprattutto fra i giovani, hanno dei rischi molto seri per la sicurezza. Non quella informatica, ma quella personale degli utenti.

WeChat non solo permette lo scambio di messaggi e immagini fra sconosciuti da qualunque smartphone (e invita attivamente a farlo, tramite la funzione Scopri), ma a differenza di altri sistemi di messaggistica indica anche a che distanza approssimativa si trova l'interlocutore, usando i dati GPS del telefonino.

È quindi facile, per un molestatore, selezionare la vittima e poi scoprire dove abita, dove lavora o dove va a scuola, facilitato nel compito dalla foto del volto pubblicata dal suo bersaglio senza pensare alle conseguenze.

Per non farsi localizzare occorre tenere spento il GPS, rinunciando però alle funzioni utili di localizzazione dello smartphone.

SnapChat, invece, promette di inviare all'interlocutore fotografie che si autocancellano dopo pochi secondi: l'ideale per scambiarsi foto ridicole, imbarazzanti o intime pensando che dopo quella fugace visione spariscano per sempre.

La promessa è vana: le immagini sono comunque recuperabili dopo la loro scadenza, sono salvabili con l'opzione "cattura schermo" (per chi ha i riflessi pronti) e per i dispositivi Apple c'è persino una app che fa tutto automaticamente: si chiama SnapHack.

La miglior difesa è dare per scontato che qualunque foto che inviamo resterà visibile per sempre e a chiunque, compresi gli ex partner vendicativi e i futuri datori di lavoro.

PAOLO ATTIVISSIMO

La Borsa *della* Spesa
Edizione 8.13

Doppioclick: La foto-estorsione corre sul web

Ultimamente i criminali stanno sfruttando Internet per compiere estorsioni particolarmente odiose, specialmente nei confronti dei minori: catturano immagini intime o imbarazzanti degli utenti attraverso la telecamerina del computer o del tablet (con appositi virus oppure fingendosi belle ragazze nelle chat video) e poi minacciano di pubblicarle, mandandole in particolare agli amici della vittima, se non verranno pagati. Tipicamente la richiesta è di qualche centinaio di franchi, da pagare di nascosto: una situazione senza vie d'uscita per molti minori, che porta talvolta a gesti estremi.

L'estorsione è facilitata da un comportamento frequente degli utenti: la visibilità pubblica dell'elenco degli amici sui social network, in particolare su Facebook. È difficile immaginarsi che dichiarare pubblicamente di chi si è amici possa comportare un rischio, ma questi ricatti dimostrano che è così.Per nascondere quest'elenco in Facebook occorre visualizzare l'elenco degli amici, cliccare sull'icona della matita e scegliere Modifica Privacy, rispondendo poi con "Solo io" alla domanda "Chi può vedere i tuoi amici?". È meglio nascondere l'elenco degli amici anche agli amici stessi, perché spesso l'amicizia (nel senso ingannevole che ha questo termine su Facebook) si concede anche a sconosciuti.

Ovviamente la prevenzione è la miglior cura: contro i guardoni che usano i virus per catturare immagini dalla telecamera del computer o del tablet servono un buon antivirus e un tappo rimovibile (per esempio un pezzo di nastro adesivo opaco) applicato sulla telecamera; contro le finte seduttrici telematiche è importante ricordare che sanno rendersi molto credibili, usando spesso delle registrazioni prese da siti erotici o addirittura assoldando delle complici che recitano dal vivo. La prevenzione passa anche attraverso l'informazione: se avete figli giovani, anche giovanissimi, avvisateli di queste trappole.

PAOLO ATTIVISSIMO