# La sicurezza informatica “fai da te” ed il furto di identità sul web

**Date :** 4 luglio 2017


## La fobia della privacy

L’utenza che utilizza *devices* elettronici portatili ha, ormai da qualche tempo, assunto un atteggiamento schizofrenico nella presunzione di poter essere sistematicamente oggetto di intercettazione della propria *privacy*.

Da qui la corsa verso apparati della “mela” dove è possibile fare l’*upgrade* all’ultimo punto di aggiornamento e, così, salvaguardare il sistema *iOS* da tentativi di *jailbreak* in grado di aprire una falla sul dispositivo; o verso quei dispositivi *Android* di alta fascia in cui il *brand* ha realizzato una piattaforma impermeabile ove sarà possibile allocare i propri dati maggiormente a rischio.

I più esigenti, per maniacalità o, altrettante volte, per logiche professionali o “criminali”, prediligeranno l’acquisto di *cryptophone* assemblati nei paesi dell’Est, o di *kit* satellitari in grado di comunicare con *Thuraya* ed *Inmarsat*.

Ecco, allora, l’impennata sui mercati della sicurezza informatica di sistemi di blindatura, a basso costo, di apparati elettronici portatili, che vanno dall’identificazione biometrica, alla cifratura di accesso con codici numerici e segni, alla custodia protetta di più cartelle con autonome *keywords* di accesso al sistema, alla foto dell’impiccione che ha provato a forzare la chiave di accesso, con una miriade di applicazioni scaricabili gratuitamente sui vari *stores*.

Una procedura isterica che vede “*il tizio*” di turno, nello stereotipato ed incontrollato meccanismo di controllo del suo *smartphone*, prima porre il dito sul *device* per ottenere il riconoscimento della propria impronta digitale, poi avviare lo sblocco di sistema con la chiave di apertura della *home* del dispositivo (oltre alle procedure di sblocco del PIN della SIM telefonica), per poi accedere, ad esempio, ad una finta cartella che all’interno contiene, tra i tanti, *WhatsApp, Telegram, Skype, Messenger* o *Viber*.

Ed, ancora, un’ interminabile procedura di *privacy*, con l’avvio dell’applicazione di interesse con un finto *crash* di sistema che rimanderà alla comparsa della dicitura “*il processo si è*

*interrotto inavvertitamente*” o, facendo scorrere due dita in basso sullo *screen*, consentire l’accesso alla pagine dell’applicazione; da qui ancora la nuova maschera di sistema con il codice di accesso (doppio su *Telegram* in modalità segreta) e finalmente accedere all’applicazione richiesta (senza poi contare la possibilità di avviare *chat end to end* con la distruzione programmata dopo un certo intervallo di tempo).

Una procedura che sa di ridicolo se si considera che ormai una buona fetta di utenza, per aumentare la *performance* del dispositivo che tiene incollato in mano, è passata all’utilizzo di macchine spinte da processori *multi core* (mediamente *quad* ed *octa core*) con memorie di sistema che ormai si sono attestate a non meno di 3 *giga* di RAM, con *storage* fino a 256 *giga*.

*Routine* che rimandano, poi, alla maniacale chiusura delle applicazioni in esecuzione, per salvaguardare (pensano gli utenti) la memoria impegnata ed il consumo di batteria: ovviamente ciò determina un nuovo protocollo isterico, con l’abilitazione di una ulteriore *password* che consente l’accesso alle *app* recenti così da poterle chiudere, per poi passare alla scansione del sistema per monitorare la presenza di *virus*, la pulizia di *files* temporanei delle pagine consultate, la “*bonifica*” di eventuali siti a contenuti “*per adulti*” visitati, e quanto altro ancora (senza contare la tante applicazioni che rimandano alle connessioni *wifi* agganciate dall’utente).

Si tratta di procedure che fanno leccare i baffi ai programmatori i quali, ancor prima di pensare alla fruibilità del loro prodotto in modalità più o meno *free*, si ingegnano su come poter creare il maggior numero di pagine pubblicitarie e di *banner* da inserire nel corso dell’avvio di quella camaleontica applicazione di tutela della *privacy*.

## Il furto di IP e d’identità sul web

L’utenza però, da un punto di vista della sicurezza informatica, non si pone, il più delle volte, il problema del furto del proprio *account*: la più banale ed insidiosa procedura che consentirà ad un *hacker* di impadronirsi del “*mondo virtuale*” di una persona con un solo *clic*.

Una prima, sciocca, procedura è quella nota negli USA con il termine *wardriving*, una sorta di gara tra piccoli geni che consisteva nel forzare l’accesso ad una connessione *wifi* protetta utilizzando, come antenna, un tubo di patatine *pringles*.

Un protocollo desueto atteso che, i più, dimenticano di attivare una protezione alla propria connessione (sia essa proveniente da una banda larga domestica o dalla condivisione *hot spot* con un dispositivo GSM), cosicché è sempre più frequente notare, in prossimità degli armadi di smistamento dei gestori telefonici, ragazzini appena sbarcati dall’ultima nave che già sono in grado di smanettare per trovare una delle tante “*porte*” aperte senza una protezione (negli *standard WEP, WPA, WPA2*) ed iniziare le loro connessioni *VoIP* con l’altro continente.

Ma accanto a questo, non sempre banale, furto di indirizzi IP, la questione ancor più delicata riguarda l’*account* dell’utente su uno dei tanti sistemi che, parallelamente, gestiscono più *devices*, contenuti *social*, cartelle di posta elettronica, nuvole di *back up* dei dati, e mille altri

effetti personali non troppo virtuali.

A detto proposito, mentre l'utente è particolarmente accorto nello sblocco del proprio *device* nascondendo il proprio segno di apertura (solitamente una zeta, una elle o una enne) o riducendo al minimo i caratteri e ad un lumicino l'intensità dello schermo, poco ricorda del proprio *username* e della *password* che consentono di accedere al proprio mondo.

Ma, ancor meno, ha memoria di aver, o meno, consentito al sistema, quale impostazione di *default*, di effettuare operazioni di *back up* sul *cloud* di *account*, di effettuare uno *streaming* del proprio rullino fotografico, di impostare la consultazione di più indirizzi di posta dallo stesso *client*, e quanto altro ancora.

Può accadere, allora, nella più banale delle ipotesi, che il consumatore stanco del proprio *smartphone, tablet* o *pc* portatile, abbia deciso di passare alla versione *plus* o di nuova generazione e di regalare o disfarsi, contestualmente, del vecchio dispositivo, senza ripristinare le impostazioni di fabbrica.

Accadrà allora che il nuovo fortunato utente, con il telefonino di seconda mano, inserita la propria sim senza aggiornare l'*accoun*t, si troverà, ad esempio, tra i *folder* della propria galleria fotografica le foto che, nel frattempo, il generoso amico ha iniziato a scattare, o le *mail* rimaste attive negli *account* di posta, i profili dei *social* (ad eccezione di *whatsapp* che non consente la simultanea fruibilità su più indirizzi telefonici, ma solo attraverso la procedura *WhatsApp Web* con l'abbinamento del *QR Code* di una diversa macchina).

Analoga criticità si configura nel caso in cui una persona, che in modo clandestino o con raggiri, si è impadronita dei privilegi di un dominio (ad esempio il marito che ha regalato il telefono alla propria signora, o il datore di lavoro che ha omaggiato la segretaria di un telefono di servizio), così da poter avere il possesso virtuale di quell'utenza.

## L'ackeraggio d'elite con i brute force seriali

Ma se queste possono essere ovvie discussioni da osteria, si consideri, invece, l'*hacker* professionista che per svariate ragioni ha interesse a vulnerare un profilo e rubarne l'identità: l'attività avrà inizio con l'individuazione dell'*account*, solitamente abbinato ad un indirizzo di posta elettronica, procedendo poi alla forzatura della *password* con un programma più o meno avanzato di *brute force* seriali, in grado di "*lavorare*" in tempi ridottissimi chiavi di apertura anche di diversi caratteri.

Ecco la ragione per cui si suggerisce di utilizzare caratteri alfa numerici molto lungi e complessi, con l'aggiunta di segni e maiuscole, così da rendere sempre più difficoltosa la forzatura del sistema.

Nella realtà accade però, il più delle volte, che la *password* di accesso sia un nome di persona abbinato ad una data (ad esempio: michele64), che renderà la procedura di accesso di una facilità disarmante.

Certo, in tal caso il “sistema”, rilevato l’accesso *sui generis*, dovrebbe in astratto inviare un messaggio di *alert* all’indirizzo preimpostato dall’utente all’atto di creazione dell’*account*: ad esempio con scritto “*nuovo accesso al tuo account da dispositivo Android-iOS…., zona Catania ore….”.*

Però il problema, il più delle volte, rimanda a quello smemorato indirizzo di posta, che è stato nel frattempo dismesso dall’utente o viene utilizzato residualmente, con accesso una *tantum* da remoto senza che, quindi, l’interessato sia in grado di accorgersi in tempo reale dell’accesso fraudolento.

Nelle attività di *intelligence* l’*iter* di infiltrazione è un tantino più complicato, a volte con il disturbo in prossimità dell’utente attenzionato, attraverso l’inibizione dei dispositivi di comunicazione con *jammers* in grado di disturbare il segnale GSM, o con la momentanea interdizione all’accesso della linea fisica che alimenta la rete *internet* domestica (dal chiostrino o dall’armadio di smistamento); ciò consentirà l’inibizione della ricezione del messaggio di *alert* o, in altri casi ancora, la veicolazione di messaggi *fake* in grado di ingannare il bersaglio.

Effettuata la penetrazione nel sistema, lo stretto necessario per effettuare le procedure di possesso, l’*hacker* avrà, poi, diversi modi per monitorare l’utente una volta abbandonata “*la presa”:* dal clone del dominio dell’*account*, all’osservazione attraverso uno *spyware*, al pedinamento con applicazioni di localizzazione, alla scansione con sofisticati ed invisibili *keylogger* in grado di memorizzare le varie *password* utilizzate dal cliente bersaglio, o molto altro ancora.

Si tratta, da un profilo giuridico, di procedure illegali che, dall*’interferenza illecita nella vita privata* (art. 615 bis cp), passano all*’accesso abusivo ad un sistema informatico o telematico* (art. 615 ter cp), alla *detenzione e diffusione abusiva di codici di accesso a sistemi informativi o telematici* (art. 615 quater cp), alla d***iffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615 quinques cp),** alla *cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche* (art. 617 cp), all*’installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche* (art. 617 bis cp), alla *falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche* (art. 617 ter cp), alla *i**ntercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617 quater cp), alla *installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche* (art. 617 quinques cp), fino alla *falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche* (art. 617 sexies cp).**

## Un banale suggerimento

In conclusione al brevissimo approfondimento sul tema della sicurezza informatica “*fai da te”*, il suggerimento all’utente rimane quello - prima di badare alla *performance* di prestazione, di attrazione estetica del proprio *device* ed all’utilizzo delle tante applicazioni che ne

appesantiranno uso e fruibilità – di considerare prioritariamente:

1. la sicurezza dei propri *account*, con chiavi di accesso complesse e differenti per ogni singolo profilo;
2. una frequente revisione di cambio *password*;
3. l'attivazione di sistemi "*sentinella*" in grado di fornire all'utente un *alert* di accesso, tramite *mail* o *sms*;
4. il controllo di tutti i *devices* collegati allo stesso *account*;
5. la disattivazione del proprio *account* in caso di cessione di un apparato e l'inizializzazione alle impostazioni di fabbrica.

Per ultimo, ma non da ultimo, per evitare che forme di *addictions* da apparato elettronico distorcano in patologie croniche, il consiglio più accorato è quello di un utilizzo dei *devices* elettronici come strumento voluttuario (quanto separabile) di ausilio nella *routine* dell'individuo, piuttosto che quale sorta di estensione bionica in grado di influenzare e, spesse volte, condizionare pesantemente il vivere quotidiano.

Se così non fosse, quella "*scatola nera*" che portiamo con noi potrebbe, una sera, farci forse ritrovare in una pantomima non troppo distante da quella pellicola di Paolo Genovese che mette a fuoco, attorno ad un tavolo nel corso di una cena, tanti "*perfetti sconosciuti*".

A cura di: **Michelangelo Di Stefano**