Smartphone Sicuro

Smartche?

Smartphone **non** più telefono

- per smartphone intendiamo un telefono che abbia capacità di calcolo e memorizzazione
- arrivano da lontano,il primo progetto è di IBM del 1992 (commercializzato nel 1993)

Siamo consapevoli di cosa ci portiamo in tasca?

(e cosa diamo in mano ai nostri figli?)

- abbiamo in mano dei veri e propri computer con delle potenze di calcolo enormi
- ormai la funzione telefono è marginale e lo vediamo anche nei piani telefonici delle compagnie: le telefonate sono gratuite, la cosa che davvero viene venduta è la banda internet
- i Sistemi Operativi tipo Android sono dei derivati di sistemi operativi dei computer (Android stesso è un Linux ottimizzato per cellulari). Se pensiamo ad Apple la differenza tra cellullare e sistema operativo è sempre più sottile (handoff/wearable)
- il telefonino ci segue ovunque e con questo strumento eseguiamo praticamente tutte le operazioni che facciamo con il computer

Che lampadina dovrebbe accendersi?

Proteggiamo i nostri computer con antivirus e protezione per la navigazione, ma generalmente non facciamo molta attenzione ai nostri cellulari.

Li consideriamo nella comune percezione ancora dei semplici telefoni.

Iniziamo da…

- PARLIAMO DI PRIVACY… questa sconosciuta

Un saggio mi raccontò che esisteva un tempo in cui la gente riusciva a mangiare senza fotografare il cibo….

Siamo protettori della privacy…

Ma scriviamo tutto di noi sui social ;)

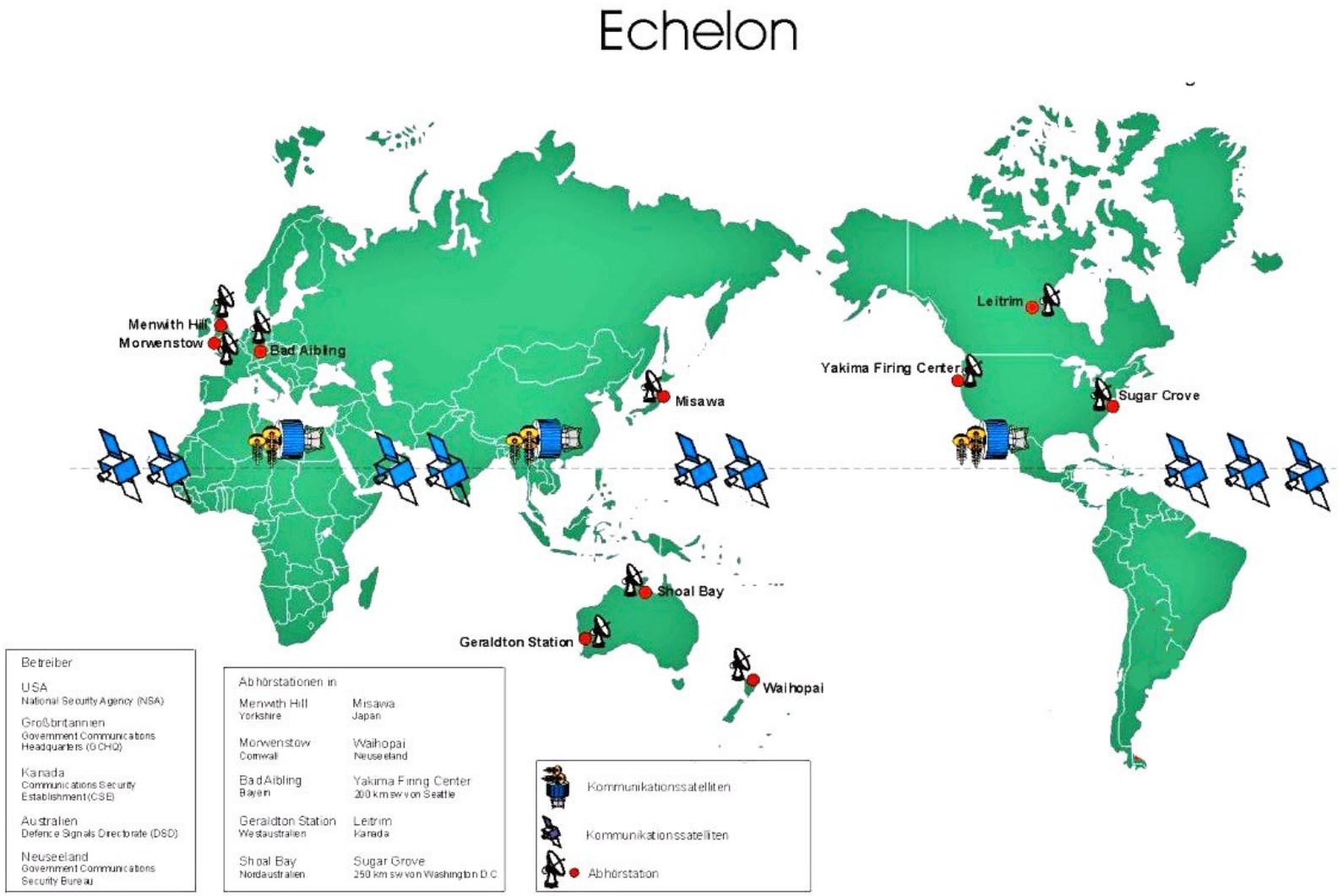
Siamo tutti intercettati?

La “mania” della Privacy è recente, parte con Prism nel 2013, ma Prism è solo il più eclatante dei c

- Echelon
- Sismi
- Prism
- Hacking team

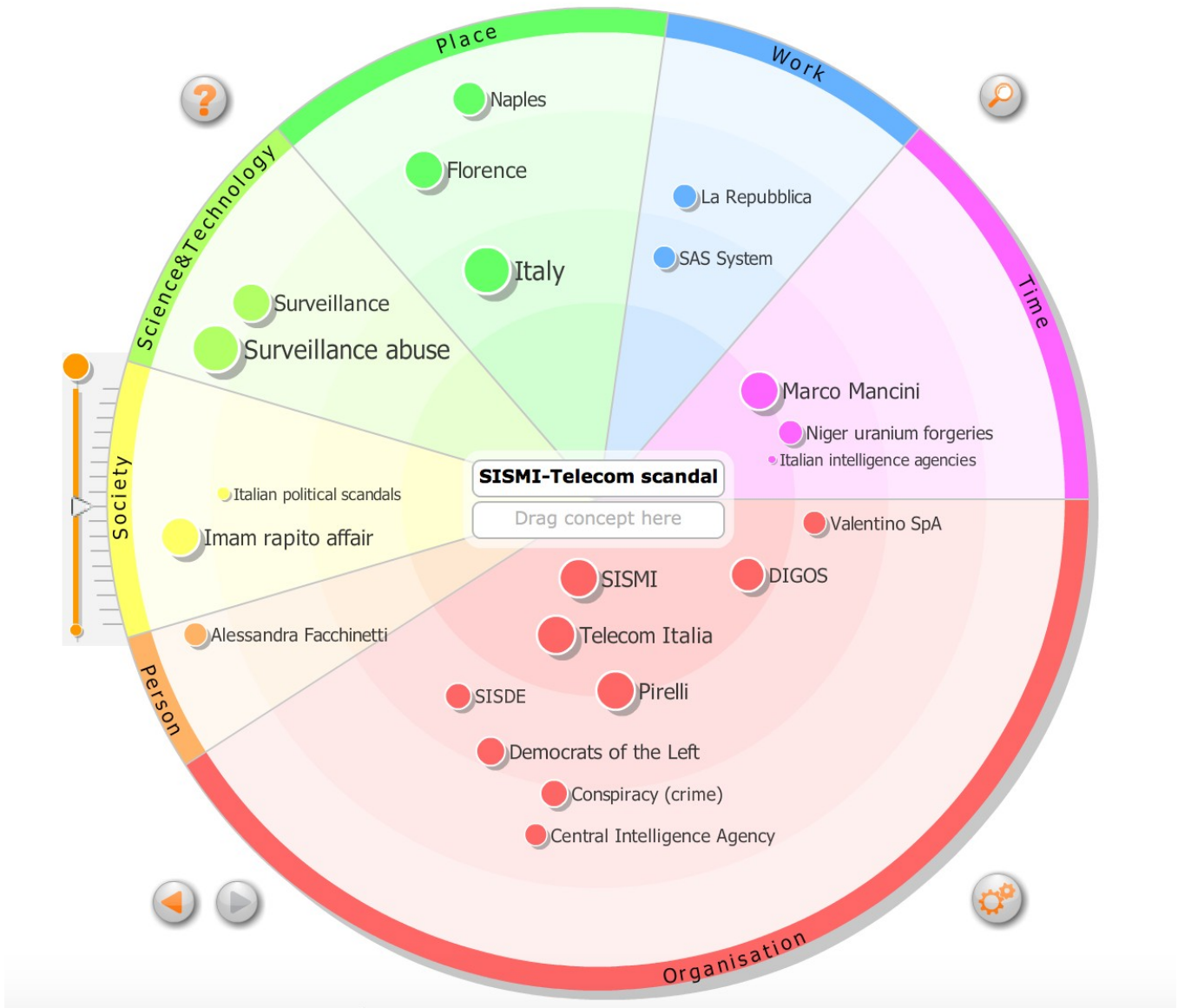
Questi sono I casi conosciuti, anche per l’abuso di sensazionalismo della stampa

Echelon



Il sistema si basava sull'intercettazione dei cavi sottomarini, con i dati che venivano replicati e inviati ai vari centri di elaborazione: Menwith Hill (Gran Bretagna), Pine Gap (Australia), Misawa Air Base (Honshu Giappone) e l'isola di Ascensione (Oceano Atlantico).
Ci sono prove che veniva usato per spionaggio industriale.
Esiste un report ufficiale del Parlamento Europeo disponibile online.
USA e NSA ne hanno sempre negato l'esistenza

Sismi



Anche noi abbiamo il nostro scandalo locale sulle intercettazioni!! (non ci facciamo mancare nulla!)
Più piccolo, limitato e fatto, sembra, per scopo di lucro, ma non si è mai capito il vero scopo.

Il caso scoppia nel 2006, ma è accertato che le intercettazioni andavano avanti dal 1996: 21 arresti, 34 rinvii a giudizio

5000 intercettati

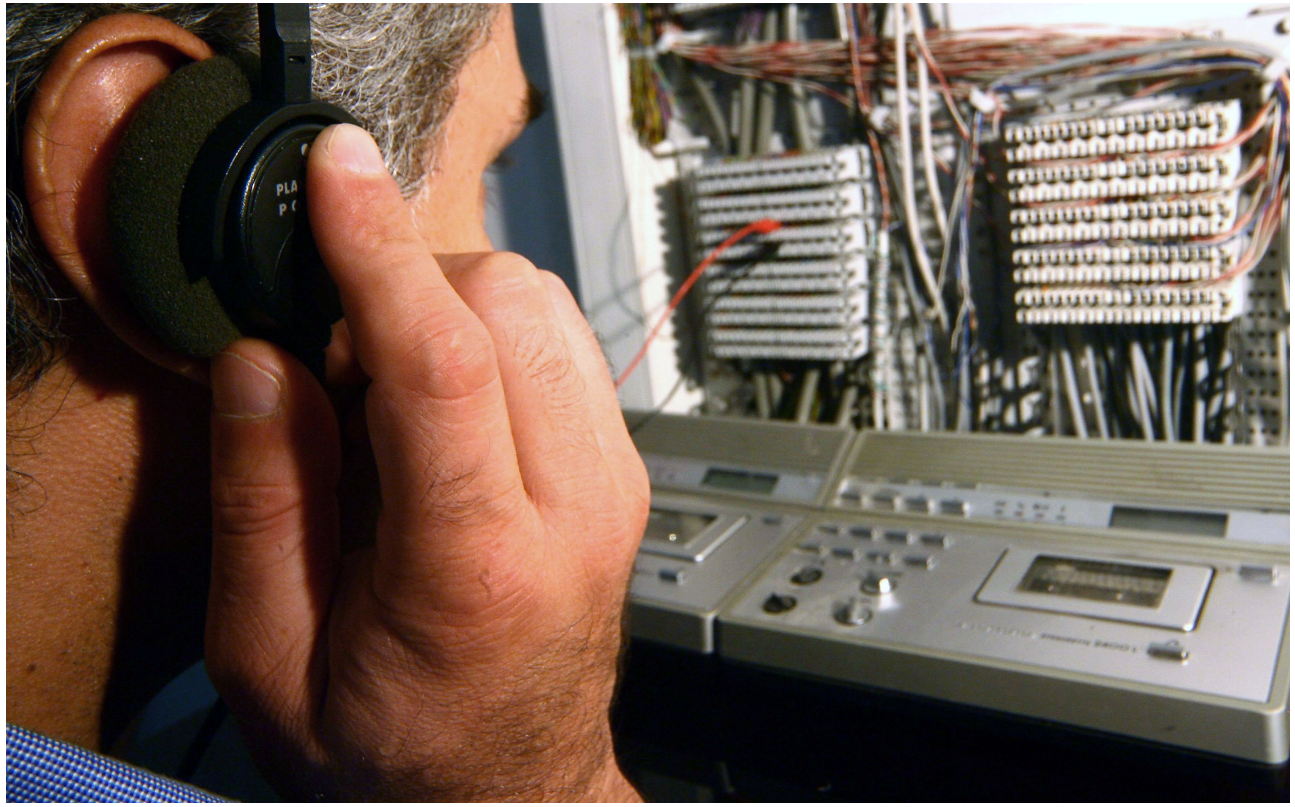
Prism, nome interno:“US-984XN”

Progetto americano, il programma fu autorizzato dalla Fisc (Foreign Intelligence Surveillance Court) per dare concretezza al “Protect America Act”.
Sembra accertata la partecipazione dell’inghilterra.
Scoperto per le dichiarazioni di Edward Snowden nel 2013.
La NSA ha sempre rivendicato la legittimità del programma.

Hacking Team

- Questo scandalo colpisce l'Italia
- Azienda milanese che vende un software spia inrilevabile, usato dalle *intelligence* di tutto il mondo
- L'azienda subisce un attacco e 400 giga di dati finiscono on line (mail, codice e dati)

Tutto questo cosa ci fa capire?



Un tempo, quando si pensava alle intercettazioni, si pensava a intercettazioni ambientali

MICROFONI

LASER PER LE VIBRAZIONI DEI VETRI

etc. etc.

Adesso l'intercettazione si è evoluta, la quantità di dati che diamo più o meno coscientemente è enorme.

Non ci si limita più alla sola telefonata/mail.

Si è evoluto anche il genere di dati

Coi cosiddetti "Big Data" si fa correlazione, non si controlla piu' solo la telefonata, la localizzazione diventa un elemento importante.

Avete notato che nell'IOS9 appare, senza che voi facciate nulla, quanto manca all'arrivo a casa? O al lavoro?

Non è più solo **Google now**!

Sapete che le funzioni di geolocalizzazione si possono disabilitare?

Si è evoluto anche il genere di dati

Un piccolo esempio di correlazione e perchè non è così irrilevante far sapere dove siamo.

Il mio cellulare si trova nella posizone X, nella stessa posizione si trova il cellare di un'altra persona Y, nessuno sta telefonando, ma questa associazione si ripete, magari ad intevalli regolari per periodi di tempo.

Potrò poi negare la mia conoscenza con questa persona?

Geolocalizzazione

Tutti gli smartphone, che siano Apple o Android o altro ancora, salvano in un log tutti i riferimenti alle posizioni rilevate dal modulo GPS. In pratica lasciamo delle tracce come Pollicino. Dove vengono saltavi questi dati? Partiamo da Apple, dall'iPhone 5. Per accedere al menu "Posizioni frequenti" andate in Impostazioni, poi in Privacy, quindi in Localizzazione. Scorrete in basso fino a "Servizi di sistema" e, nel sottomenu, cercate "Posizioni frequenti". Qui trovate elencati tutti i vostri spostamenti. Potete cancellare la cronologia e, apparentemente, impedire le prossime rilevazioni: in realtà gli spostamenti vengono comunque registrati, sfruttando i ripetitori WiFi. Per smartphone Android c'è una sola app per visualizzare questo log, ma richiede il rootkit. Si chiama "Location Cache" ed è realizzata da Remydemy

Esagero? Forse no..

Viviamo una vita sui Social, e i nostri figli più di noi, ma siamo coscienti di cosa condividiamo e con chi?

Parliamo di una cosa sconosciuta ai più

L'**EULA**

End **U**ser **L**icence **A**greement

Eula (scusate ma questa vale la pena leggerla [illegible]eme)

I contenuti dell'utente nei nostri Servizi

Alcuni dei nostri Servizi consentono di caricare, trasmettere, memorizzare, inviare o ricevere contenuti. L'utente mantiene gli
eventuali diritti di proprietà intellettuale detenuti su tali contenuti. In breve, ciò che appartiene all'utente resta di sua proprietà.

Quando l'utente carica, trasmette, memorizza, invia o riceve contenuti da o tramite i nostri Servizi, concede a Google (e ai
partner con cui collaboriamo) una licenza globale per utilizzare, ospitare, memorizzare, riprodurre, modificare, creare opere
derivate (come quelle derivanti da traduzioni, adattamenti o altre modifiche apportate in modo tale che i contenuti funzionino al meglio con i nostri Servizi), comunicare, pubblicare, eseguire pubblicamente, visualizzare pubblicamente e distribuire i suddetti contenuti. I diritti che concede con questa licenza riguardano lo scopo limitato di utilizzare, promuovere e migliorare i nostri Servizi e di svilupparne di nuovi. Questa licenza permane anche se l'utente smette di utilizzare i nostri Servizi (ad esempio nel caso di una scheda di attività commerciale aggiunta a Google Maps). Alcuni Servizi potrebbero offrire modalità di accesso e rimozione dei contenuti forniti a tale Servizio. Inoltre, in alcuni dei nostri Servizi sono presenti termini o impostazioni che restringono l'ambito del nostro utilizzo dei contenuti inviati a tali Servizi. È necessario assicurarsi di disporre dei diritti necessari per concederci questa licenza rispetto a qualsiasi contenuto inviato ai nostri Servizi.

I nostri sistemi automatizzati analizzano i contenuti dell'utente (incluse le email) al fine di offrire funzionalità dei prodotti rilevanti a livello personale, come risultati di ricerca personalizzati, pubblicità su misura e rilevamento di

Eula

Un aneddoto divertente sempre su Google e Gmail.

Un tempo Gmail faceva la distinzione tra:

domenico.martini@ gmail.com

e

domenicomartini@ gmail.com

Non più! Credo in base all'anzianità dell'account ha stabilito la proprietà di una mailbox rispetto ad un'altra.

Ricevo mail dall'ordine avvocati, da banche e dall'ENEL per questa simpatica modifica.

Richiesta di copia fatture - Cliente: [redacted]

Inbox x

Enel <CC.ENEL.ESERCIZIO@enel.it>
to me

Sep 3

Italian > English Translate message Turn off for: Italian

Gentile Cliente,

in merito alla sua esigenza di ricevere copia della fattura della sua fornitura le confermiamo l'invio,
in allegato, della documentazione richiestaci.

L'occasione ci è gradita per cordialmente salutarla.

SERVIZIO CLIENTI
"Le fatture inviate tramite email saranno quelle certificate fiscalmente"

Ristampa della bolletta fattura n° 597456450003044 emessa il 09/07/2015. Gli elementi fiscali indicati nel documento coincidono con quelli riportati dalla società nelle distinte meccanografiche di fatturazione ex D.M. 24/10/2000, n. 370.

Enel

CASELLA POSTALE 1100
85100 POTENZA

ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: [redacted]
Codice POD: [redacted]
Partita IVA: [redacted]
Codice Fiscale: [redacted]

[redacted]
03043 CASSINO

CONTATTI UTILI

SERVIZIO CLIENTI

Punto Enel
(scopri quello più vicino su www.enelservizioelettrico.it)

www.enelservizioelettrico.it

800 900 800 Numero verde gratuito
da tutti i numeri fissi nazionali tutti i giorni, 24 ore su 24
199 50 50 55 a pagamento dai cellulari
al costo applicato dal suo operatore, tutti i giorni 24 ore su 24
Casella Postale 1100 - 85100 Potenza
per informazioni e reclami scritti

GESTIONE GUASTI

Comunicare sempre il Codice POD: [redacted]

Per segnalazione guasti:
Chiamare **803 500** Numero verde Enel Distribuzione
da rete fissa e da cellulare tutti i giorni 24 ore su 24

Per Informazioni sui guasti:
- inviare **sms** con il Codice POD al numero **3202041500**
- scaricare gratuitamente l' **APP Guasti Enel**

BOLLETTA PER LA FORNITURA DI **ENERGIA ELETTRICA**

N. fattura [redacted] del 09/07/2015 Mese **giugno 2015**

Totale da pagare entro il 29/07/2015: **euro 24,35**

Le sue bollette precedenti già scadute ci risultano pagate. Grazie

In allegato trova il bollettino per il pagamento.

Non siete ancora convinti?

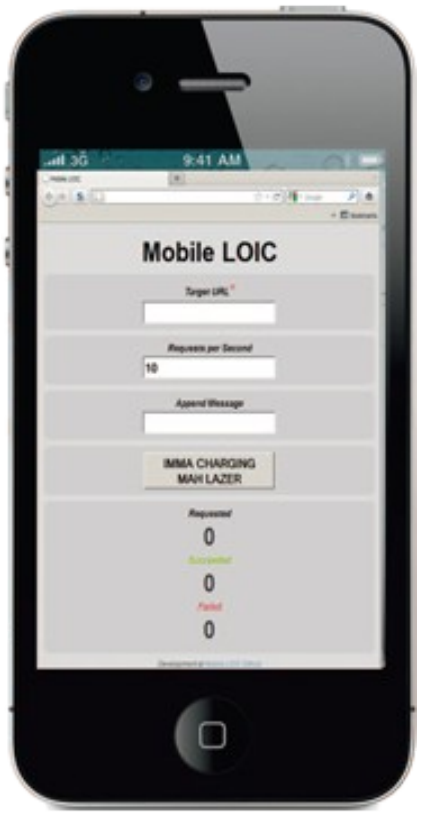
McAfee Labs ha pubblicato uno studio sul valore nel black market di alcuni dati:

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Software-generated	$5–$8	$20–$25	$20–$25	$21–$25	$25–$30
With Bank ID Number	$15	$25	$25	$25	$30
With Date of Birth	$15	$30	$30	$30	$35
With Fullzinfo	$30	$35	$40	$40	$45

I dati di un conto bancario coi codici dispositivi arrivano anche a 1000$

Attenzione, rubarvi i soldi è solo uno dei fini dell'operazione, molto più interessante è far girare dei soldi magari frutto di altre truffe.

Cercano solo i miei dati?



DOS/DDOS

- *Si legge spesso sui giornali di attacchi di tipo DOS da parte di gruppi di Aktivist o Anomymous , non bisogna pensare al sistema operativo DOS , è un acronimo per Denial Of Service. Cosa significa? Un attaccante cerca di impedire la fruizione di un servizio saturando le risorse del sistema che lo eroga.*
- *Sapevate che con le potenze in gioco oggi coi cellulari, una volta preso il controllo del vostro apparecchio possono usarlo per utilizzare un attacco di questo tipo?*

LOIC = Low Orbit Ion Canon

Vi spavento solo un altro po', poi vediamo cosa si può fare per cercare di proteggersi

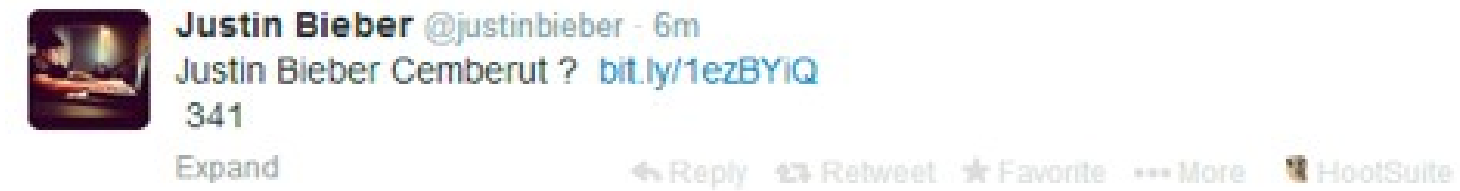
Parliamo un secondo ancora di Social

Ci sono persone/aziende con un grosso numero di persone che li segue e che conseguentemente influenzano il comportamento di milioni di persone.

Vi sembra un'esagerazione? Ci sono studi che dimostrano che se venissero compromessi gli account di Twitter dei 10 broker più seguiti d'America e pubblicassero notizie falsate ad hoc si potrebbe indurre una crisi economica come quella del 1929.

Justin Bieber il più bersagliato

8 Marzo 2014



La frase vuol dire "Justin Bieber scontroso?"

4 Maggio 2013

"E!" e' un canale televisivo specializzato in intrattenimento con un audience solo in america di oltre 96 milioni di persone e più di 6 milioni di seguaci su twitter.

il link puntava ad un App dal nome "ShootingStarPro" che era in realta' un virus.
Le persone che seguono Bieber su Twitter sono piu' di 50 milioni.

Il tweet sosteneva che Bieber fosse gay e c'era un link non funzionante ma e' abbastanza significativo che in meno di 10 minuti oltre 1000 persone lo avessero riportato (in gergo ritwittato) e oltre

Stanno solo giocando?

Il 23 aprile 2013 è stato violato l'accout Twitter della Associated Press (AP). Ed è stato pubblicato il seguente tweet.

AP si accorge e smentisce in meno di 20 minuti ed informa di essere stata bucata. Il Corriere della Sera pubblicò la notizia sul sito nei flash in home page.

Ecco il grafico Dow Jones di quel giorno

Quindi?

Facciamo attenzione!

Non sempre le persone con cui interagiamo on line anche con i sistemi di messaggistica sono chi dicono di essere.

La questione diventa particolarmente importante se pensiamo ai ragazzi

Ultima nota sui social (poi smetto giuro)

- La prima raccomandazione molto banale è di fare attenzione a cosa pubblichiamo, dire al mondo che siamo in ferie a chilometri di distanza potrebbe essere un'informazione preziosa per dei malintenzionati che vogliono fare una visita indesiderata alla nostra casa (e ci sono già stati casi in cui le assicurazioni non hanno pagato a causa di questo)
- Oltre al problema pratico dei furti esistono problemi di responsabilità.
- Ci sono stati casi eclatanti di licenziamenti di persone che si sono lamentate del lavoro su Facebook e persone che sono state querelate e sono state costrette a pagare multe per aver parlato male dei superiori

  Questo anche perchè sui social networks non siamo anonimi, ma siamo comunque rintracciabili e responsabili delle nostre azioni.
- Se consideriamo che i nostri figli sono dei grandi utilizzatori di queste tecnologie, diventa un dovere spiegare loro che non si può scrivere qualunque cosa sui social. A riguardo pensiamo ai problemi di bullismo che si sono verificati anche in Italia.

Qualche regola base

Il PIN

Usiamo sempre un PIN, ed una password, che blocchi il terminale quando va in stand-by (il PIN della SIM non c'entra): in caso di smarrimento o furto si può bloccare il sistema da remoto, ma il tempo che impieghiamo per raggiungere un computer connesso alla Rete può essere fatale.

Molti terminali (vedi Samsung e LG) supportano già il riconoscimento facciale e dall'iPhone 5S anche lo sblocco del terminale con impronta digitale (Touch ID).

Qualche regola base

Segniamoci l'IMEI

Una buona norma, quasi sempre trascurata dagli utenti, è copiare l'IMEI (International Mobile Equipment Identity) del telefono e conservarlo. In caso di furto o smarrimento, serve per bloccare il terminale e renderlo inutilizzabile, quantomeno sul territorio nazionale, anche se si cambia la SIM. Va detto, però, che un operatore può risalire al nostro IMEI analizzando i numeri chiamati.

SIM e minorenni

Nonostante la maggior parte dei negozi venda SIM a minorenni chiedendo semplicemente la carta d'identità, in teoria servirebbe la firma dei genitori. Gli operatori prevedono, in caso d'uso da parte dei ragazzi non ancora maggiorenni, il blocco automatico dei servizi a contenuto sensibile. Questo blocco può essere richiesto dai genitori.

Qualche regola base

Il Bluetooth

Il Bluetooth, vale a dire quel sistema senza fili che sfrutta le onde radio per trasmettere dati tra computer e telefoni, o tra gli smartphone, è una delle vie migliori per contagiare ed essere contagiati da malware. **Il modo migliore per proteggersi è quello di configurare il Bluetooth del cellulare in modalità "invisibile" o "non rilevabile".**

WI-fi Pubbliche

Quando ci colleghiamo a una Wi-Fi pubblica, un malintenzionato potrebbe entrare in possesso della nostra password di posta elettronica e usarla, per esempio, per mandare spam o virus, oppure potrebbe sottrarre dati sensibili.

Un suggerimento. Ricordiamoci di cancellare le reti Wi-Fi a cui ci siamo collegati in un momento di bisogno e disabilitiamo l'opzione di connessione automatica alle reti senza fili sconosciute.

Qualche regola base

Autenticazione a due fattori. Funziona in questo modo: viene prima chiesta la password standard legata all'account e, subito dopo, una password "usa e getta", generata al momento o da una app o ancora inviata via messaggio al device. Più o meno quel che avviene con tutti i servizi di home banking.

Su iPhone l'autenticazione in due step riguarda tanto gli acquisti su iTunes e App store che l'accesso ad iCloud. Ogni volta che, per esempio, si cerca di accedere alla nuvola della Mela da un nuovo device, occorre inserire password e un secondo codice temporaneo, che si riceve sul telefonino. Per abilitare questo strumento, basta andare sul sito Apple e, all'interno della sezione "My Apple ID", selezionare "Gestisci il tuo ID Apple", effettuare l'accesso e attivare lo strumento nella sezione relativa alla sicurezza.

Anche Google ha una procedura per l'autenticazione in due passaggi: prevede l'uso dell'app Google Authenticator (disponibile, oltre che per Android, anche per iOS e BlackBerry) che genera, anche in questo caso, una password temporanea. Sui sistemi Windows si può usare lo strumento "Password app".

Messagistica

Con l'avvento dei GSM e' stata introdotta la possibilità di mandare anche messaggi di testo, i famosi SMS, quasi sempre gratuiti, e gli MMS a pagamento, da cui i vari software alternativi che utilizzano altri protocolli.
Non esiste una vera app migliore di un'altra ma semplicemente quella su cui troviamo il maggior numero di persone con cui dobbiamo scambiare messaggi.

Abbastanza interessante è la questione Whatsapp, acquisito recentemente da Facebook.
Questo software era di fatto diventato uno standard per mandare SMS e foto a fronte di un canone annuale irrisorio.
L'acquisizione da parte del gruppo di Zuckerberg ha fatto sì che parecchie persone contrarie ai social media fuggissero verso altre piattaforme.
La paura maggiore degli utenti è che Facebook possa, grazie al servizio di messagistica, accedere alla rubrica telefonica per un suo uso. La cosa per altro è possibile poichè tutti i software di messaggistica

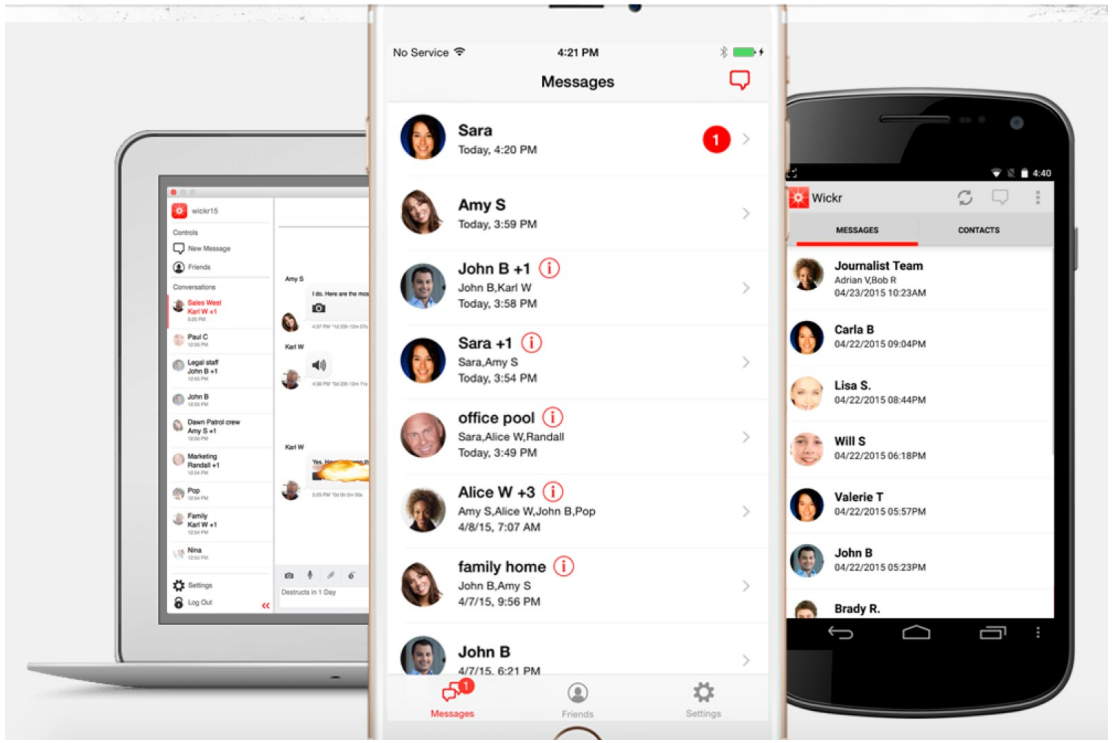
Oggi comunque Whatsapp la fa da padrone nella messaggistica alternativa. La paura è passata (?)

Messaggistica: Cosa possiamo fare?

Ci sono parecchie soluzioni per mandarsi messaggi “sicuri”

Tra i tanti, suggerisco l’open source Telegram. Fa le stesse cose di WhatsApp, con la differenza che permette di usare “secret chat” crittate con autodistruzione dopo un periodo predeterminato. I messaggi sono salvati in Cloud: questo significa che le nostre conversazioni sono disponibili anche se cambiamo terminale e che possiamo accedervi ovunque ci sia un connessione alla Rete.

Messaggistica: Cosa possiamo fare?

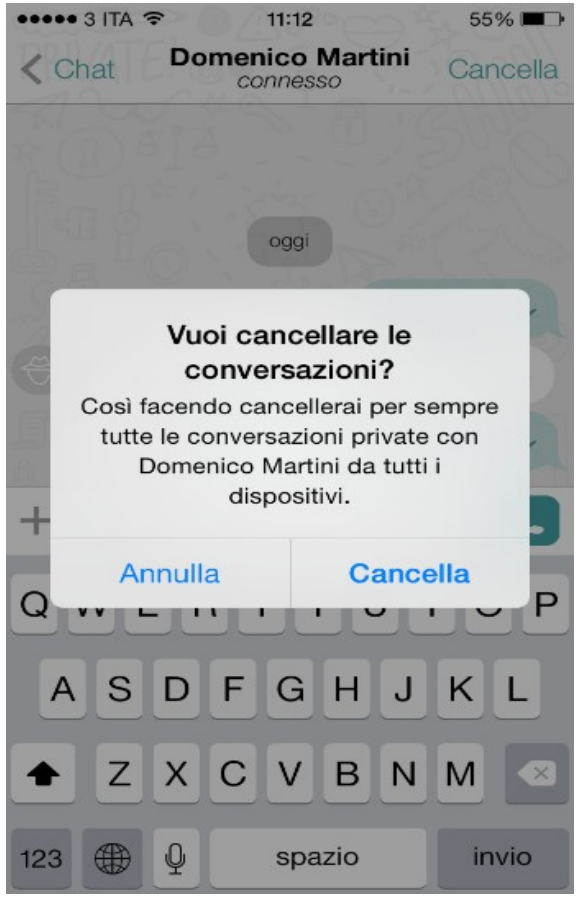


E' una app disponibile per Android, iOS, Mac, Linux e Windows.

Wickr dichiara di rimuovere qualunque dato intentificativo e geotag dai messaggi e file inviati attraverso l'app. Permette, con un solo tasto, di cancellare tutte le conversazioni e file associati dal dispositivo.

Una cancellazione che, a detta degli sviluppatori, è senza possibilità di ripensamenti

Messaggistica: Cosa possiamo fare?



Applicazione degna di nota è Wiper, anche in questo caso disponibile sia per iOS che per Android: non pone l'accento sulla sicurezza ma sul fatto che un utente possa decidere di cancellare la conversazione. L'app, per funzionare, chiede l'accesso alla rubrica: operazione comune per tutte le app di messaggistica. A questo punto siete pronti per mandare messaggi "sicuri". Ma soprattutto siete pronti per cancellarli: la cancellazione avviene sul proprio dispositivo e, soprattutto, anche su quello del destinatario.

Cosa possiamo fare?

Esistono molte soluzioni per criptare le nostre comunicazioni

Un'interessante soluzione per criptare messaggi e telefonate viene dalla società Speeka, con la soluzione CRYPTO.

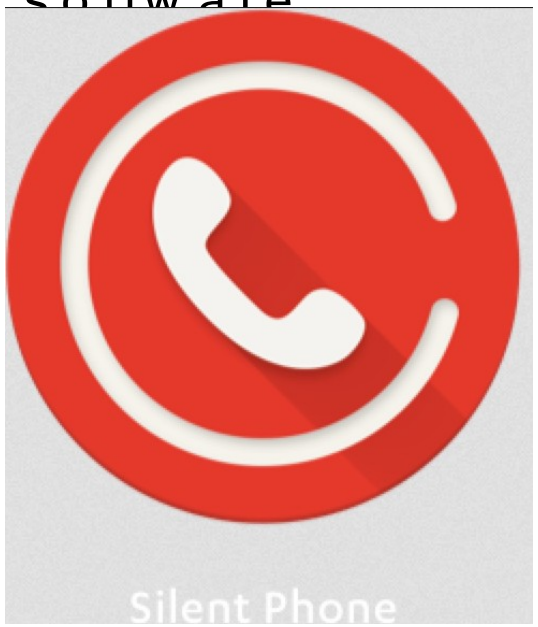
La soluzione si basa su una micro SD da inserire nel cellulare, la card non ha solo della memoria ma contiene un chip criptografco dedicato.

Per funzionare questa soluzione necessita ovviamente che tutti gli interlocutori siano in possesso della mic grosso vantaggio è che essendo una micro ò spostare tra apparati.

Cripta
voce/SMS/dati

Cosa possiamo fare?

Oltre al dispositivo da attaccare al telefono esistono soluzioni software



L'app Silent Circle, creata dall'ideatore del celebre PGP, rende possibile conversare, videochiamare, inviare SMS o email in tutta sicurezza. Questa applicazione, che permette di comunicare anche via VoIP, funziona non solo sotto rete Wi-Fi, ma se la banda è sufficiente anche in 3G e 4G, quindi ovunque. I comandi sono in tutto e per tutto simili a quelli del proprio telefonino: la praticità è garantita, il meccanismo di criptazione, cioè di protezione, è completamente trasparente per chi lo usa. I messaggi non solo vengono criptati ancor prima di lasciare il telefono, ma anche distrutti dopo un arco di tempo impostabile a piacere.
L'app non è gratuita, richiede il pagamento di un canone, oltre a ciò permette di acquistare e regalare speciali "tessere regalo", chiamate Ronin, che permettono ai nostri amici e parenti di comunicare con noi.

PGP Pretty Good Privacy. È un programma, ideato da Phil Zimmermann nel 1991, per criptare e decriptare i dati. Si basa su chiavi pubbliche e private e sulla conoscenza tra gli interlocutori.

Cosa possiamo fare?

Nel settore degli strumenti di protezione della privacy spicca anche la proposta di Whispersystem.

Signal

Interessante per due motivi.

1. Primo: l'azienda è stata acquisita da Twitter.
2. Secondo: il loro software non solo è gratuito, ma è anche open source. (significa che si può mettere le mani nel codice sorgente e renderlo eseguibile in autonomia)

Altri pro più "concreti"? Si basa sulla rubrica telefonica e permette di passare alla modalità crittata delle comunicazioni durante la chiamata.

Cosa possiamo fare?

- “Alziamo la posta” ci sono telefoni progettati come sicuri!

Sempre da SilentCircle Blackphone 2

Il sistema operativo è un derivato di Android chiamato Silent OS.

Permette di creare fino a quattro telefoni virtuali sullo stesso apparecchio totalmente separati l’uno dall’altro, separando quindi lavoro da vita privata.

Ha all’interno un software che controlla la sicurezza delle reti WiFi e l’app Silent Circle.

La navigazione è resa anonima con una VPN che il telefono instaura con i server SilentCircle

Cosa possiamo fare?

FreedomPop

Privacy Phone (detto “Snowden Phone”)

FreedomPop, azienda che si occupa di connettività ad alta velocità in modalità wireless, ha prodotto il “Private Phone”. Questo telefono, in grado di crittare tutte le chiamate e gli SMS con una chiave a 128 bit, fornisce una VPN a ogni utente, per premettere la navigazione anonima. Permette inoltre di cambiare il numero di telefono quando si vuole. Una curiosità: il prodotto può essere pagato in BitCoin.

Navigazione anonima

Ovvero fa sì che il browser non memorizzi nella cronologia i siti aperti, le ricerche e, soprattutto, i cookie dei siti visitati

Navigazione anonima su iPhone

Dalla versione 5 del sistema operativo iOS diponibile in Safari

Selezionate il tasto “Apri nuova scheda”, che si trova in basso a destra, quindi fate tap su “Privata”, in basso a sinistra.

Navigazione anonima su Android

La modalità di navigazione anonima, detta anche in incognito, è attivabile su qualsiasi browser, da Chrome a Firefox.

Navigazione anonima su Windows Phone

E’ disponibile la funzione “InPrivate” dalla versione del sistema operativo 8.1

Una volta avviato il browser web clicca sulla sinistra della barra degli indirizzi su una nuova tabs, clicca sui tre puntini in basso sulla destra per visualizzare altre opzioni e tocca su InPrivate.

Criptare un device Android

La parola crittografia deriva dal greco e letteralmente significa “scrittura nascosta”. È, in pratica, lo studio dei metodi per rendere un messaggio illeggibile se non al legittimo destinatario.

Android integra degli strumenti per fare in modo che, senza digitare un codice all’accensione, il terminale non funzioni. Si raccomanda di eseguire un backup completo e di installare l’ultima release del sistema operativo, per ridurre l’eventualità che bachi dei vecchi sistemi compromettano la criptazione. Ultima premessa: eseguite l’operazione con la batteria totalmente carica; il processo, che dura più di un’ora, non deve interrompersi per nessun motivo.
Prima di iniziare bisogna impostare un PIN o una password, rinunciando quindi al comodo unlock con gesture.
Per avviare la crittografia bisogna andare in Impostazioni/Sicurezza/Crittogafia dispositivo.
Durante la crittazione viene visualizzato il classico logo di Android a forma di ingranaggio con l’avanzamento del processo di cifratura.
Ad ogni riavvio dell’apparato sarà richiesta la password. Le performance dello smartphone peggioreranno dato che la criptazione utilizza risorse della CPU.

Sintomi preoccupanti

A volte non serve chissà quale software per scoprire che abbiamo un problema. Basta fare attenzione ad alcuni comportamenti anomali dello smartphone.

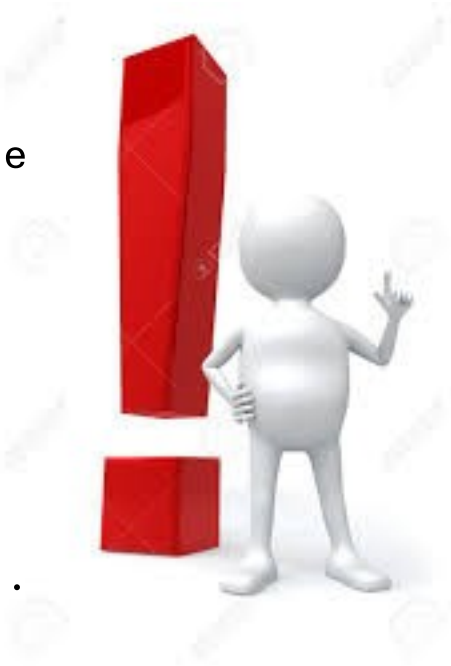
- **Durata della batteria**. Se ci rendiamo conto che improvvisamente la durata della batteria si è accorciata drasticamente, un malware potrebbe essere in attività in background.
- **Crash di applicazioni**. Se il cellulare crasha o si blocca improvvisamente, o se alcune applicazioni stabili all'improvviso impazziscono, aprendosi e chiudendosi da sole, anche in questo caso ci potrebbe essere lo zampino di un malware.
- **Chiamate internazionali o strani messaggi**. Se nell'elenco delle telefonate in uscita ci sono chiamate internazionali o comunque verso numeri sconosciuti, oppure strani messaggi di testo, occhio!
- **Addebiti strani**. Controlliamo la bolletta, addebiti strani o sconosciuti sono un altro campanello d'allarme.

Prima di parlare di virus/malware

- "app" è l'abbreviazione della parola "application", applicazione. Ogni sistema operativo mobile ha un suo "negozio", store o marketplace.
- Apple ha un controllo all'origine sul software, per cui si è "più sicuri" (ma soprattutto nello store cinese si sono verificati più casi di software infetto)
- Windows Phone: l'unico store disponibile è Windows Phone Store
- Android è una giungla! Marketplace ufficiale ora noto come Google Play. Vi sono diversi store per scaricare le app, per esempio gli store dei singoli produttori hardware: vedi il "Samsung apps". Inoltre molti sviluppatori, per non pagare la licenza a Google, pubblicano su store alternativi, per così dire privati.

Prima di parlare di virus/malware

- Evitiamo gli store non ufficiali
- Non "jailbreakiamo" I nostri terminali
- Facciamo attenzione ai permessi richiesti dalle applicazioni: perché l'applicazione torcia dovrebbe chiedere permessi per accedere al sensore GPS?
- Ho l'iPhone, posso stare tranquillo? SI e NO
  Esiste un exploit chiamato Masque: arriva una mail che invita ad un aggiornamento con un link. Seguendolo si viene avvertiti che si sta installando un'applicazione (ma chi legge davvero? E il nome è uguale all'app della mail...), nel processo vengono sostituite anche altre app (es. Gmail e quindi il telefono risulta compromesso)
- Diffidate anche dai telefoni cloni low cost. Sapevate che lo Star N9500, un clone low cost di Galaxy S4, diffusissimo in Cina, aveva preinstallato un malware?



Virus/Malware

Due milioni di minacce

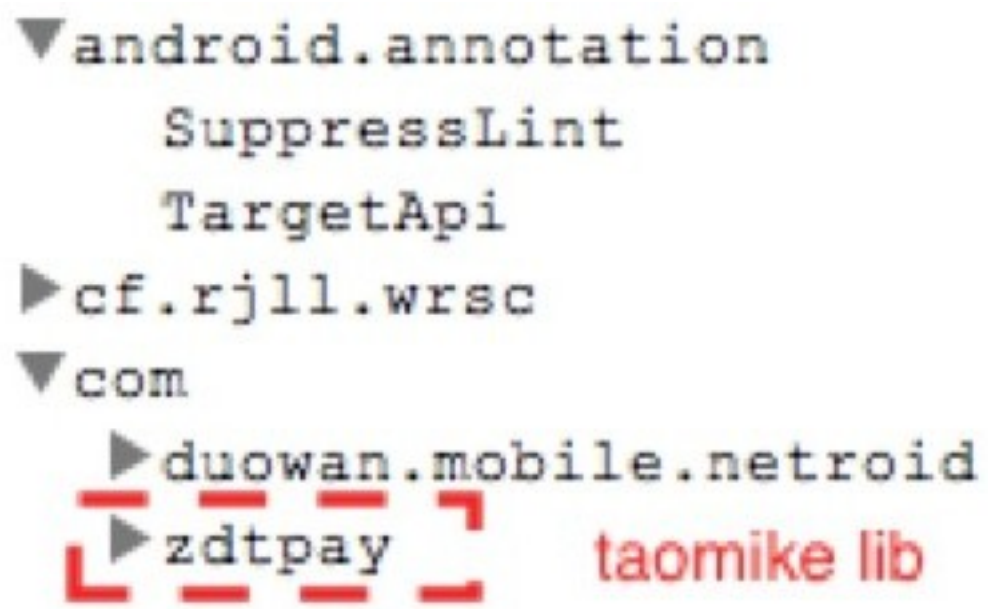
Secondo Trend Micro le minacce mobile continuano a crescere: hanno raggiunto il record di due milioni a fine marzo 2014.

Vanno dai cavalli di troia (applicazioni che permettono di prendere il controllo dell'apparato) a virus distruttivi a keylogger (che sui cellulari si chiamano taplogger).

Esistono i virus inseriti in "buona fede":

-La compagnia Cinese Taomike ha distribuito gratuitamente un kit di sviluppo, con all'interno un malware che copiava tutti gli SMS.

Risultato? → **18000 applicazioni virate sul mercato!**



Cosa possiamo fare?

Come ogni malattia anche il virus informatico ha la sua medicina, con dei distinguo, tra iOS e gli altri sistemi operativi.

Presenterò alcuni prodotti significativi ma c'è solo l'imbarazzo della scelta.

Nessun software o device è in grado di escludere al 100% ogni minaccia o pericolo

Secondo uno studio dell'azienda Fireeye esistono sul mercato diversi prodotti antivirus assolutamente inutili, che si limitano a mostrare rassicuranti pallini verdi senza in realtà proteggerci (alcuni anche a pagamento).

Cosa possiamo fare?

Non esistono sullo store Apple antivirus
A meno di Jailbreak quindi non è possibile installarne

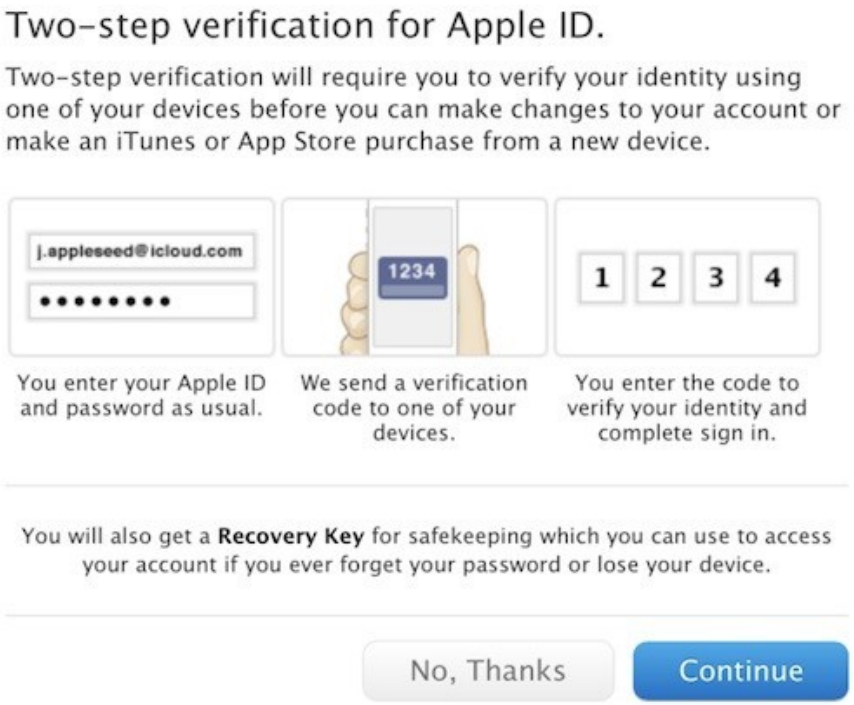
Come detto la maggior parte degli attacchi sui cellulari arrivano da malware, se il sistema Apple anche per la sua caratteristica di sandboxing è dichiarato sicuro, possiamo lavorare sulla navigazione!

Sandbox: ogni applicazione viene eseguita in uno spazio isolato dalle altre, non c'è possibilità di scambio di dati

Sapevate che le impronte digitali e le password sono salvate criptate in area separata del sistema operativo e non è possibile decriptarle neanche da parte di Apple?

Cosa possiamo fare?

Come ho detto prima le password sono critpate sul telefono… a meno che non decidiate di usare il keychain su iCloud. In quel caso USATE LA DOPPIA AUTENTICAZIONE già discussa



Con la doppia autenticazione applicata ad iCloud non sarebbero stati possibili i casi di furto di foto accaduti a un po' di personaggi famosi gli anni scorsi

Cosa possiamo fare?

"NATIVI DIGITALI" ovvero i nostri figli

Secondo Netsafe, le maggiori preoccupazioni dei genitori sono quelle di riuscire a controllare, se non bloccare, le seguenti funzioni dei telefonini:

- uso della videocamera;
- black list, ovvero il blocco di chiamate e SMS da alcune persone;
- poter restringere l'uso a certe ore e limitare l'uso di Internet, come sul PC;
- bloccare il file sharing e l'installazione di app.

Non parlerò dei vari cellulari oggi in vendita dedicati ai bambini, ce ne sono parecchi.

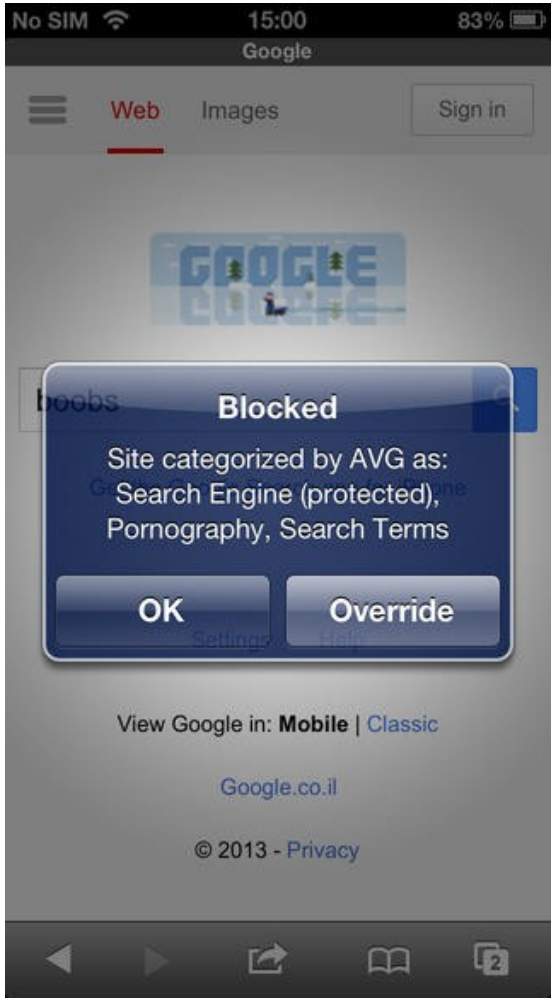
Cosa possiamo fare?

iOS include una sorta di “parental control”, per quanto con funzionalità base. Questo permette di limitare l’accesso ad alcune app o funzioni (per esempio la fotocamera) e impedire l’accesso alle app per fascia di età. Consente anche di bloccare la riproduzione di video e musica, scelta a seconda del rating o di “explicit lyrics”, di materiale esplicito. Permette anche il blocco della navigazione Web, agendo su siti per adulti in generale o su siti preimpostati.

Cosa possiamo fare?

Dal punto di vista del parental control puro, Windows Phone 8 è decisamente avanti: consente livelli di controllo preimpostati a seconda dell'età dei ragazzi: vedi l'angolo dei bambini. Permette anche di bloccare le app dal sito Web del sistema mobile.

Cosa possiamo fare?



Per dare in tranquillità il vostro iPhone/iPad/Windows Phone ai vostri figli AVG Family Safety. Si tratta di un browser Web, che consente di bloccare siti Web inappropriati, offrendo protezione contro truffe, frodi, phishing e contenuti online potenzialmente dannosi. Inoltre la funzionalità Do Not Track, segnala i siti Web che raccolgono informazioni sulle attività online dell'utente, che può scegliere se consentirli o meno. Family Safety permette di proteggere le impostazioni con un PIN di 4 cifre. Una nota: con questo nuovo browser in funzione, occorre bloccare Safari.

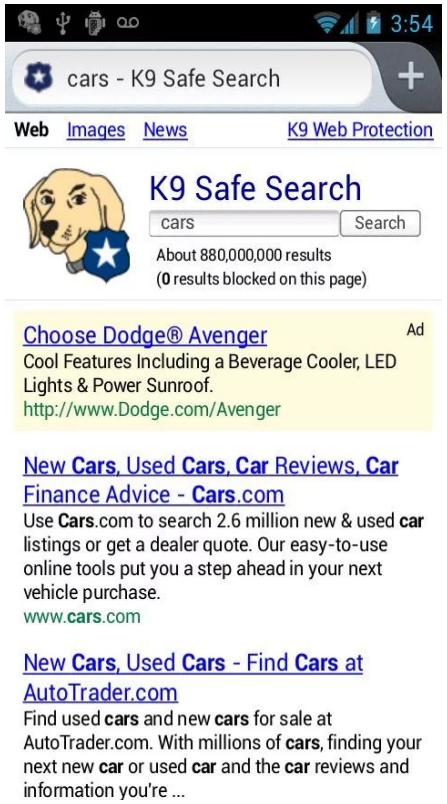
Basta entrare nelle impostazioni del sistema e andare in "Generali". In "Restrizioni", dopo aver impostato un codice di quattro cifre per accedere all'area, basta scegliere di bloccare Safari. Così il browser non comparirà più in iOS.

AVG per Android propone un antivirus gratuito

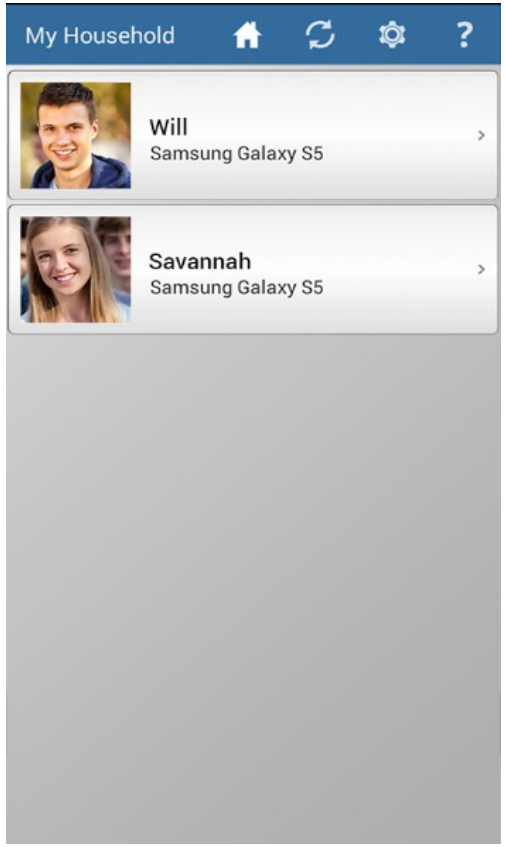
Cosa possiamo fare?

Per il cosiddetto parental control esistono parecchie applicazioni, da quelle che inibiscono solo certi contenuti a quelle che creano una copia di tutte le attività del telefonino.

Controllare è spesso necessario, ma consiglio comunque di parlare e informare i vostri figli dei pericoli possibili.

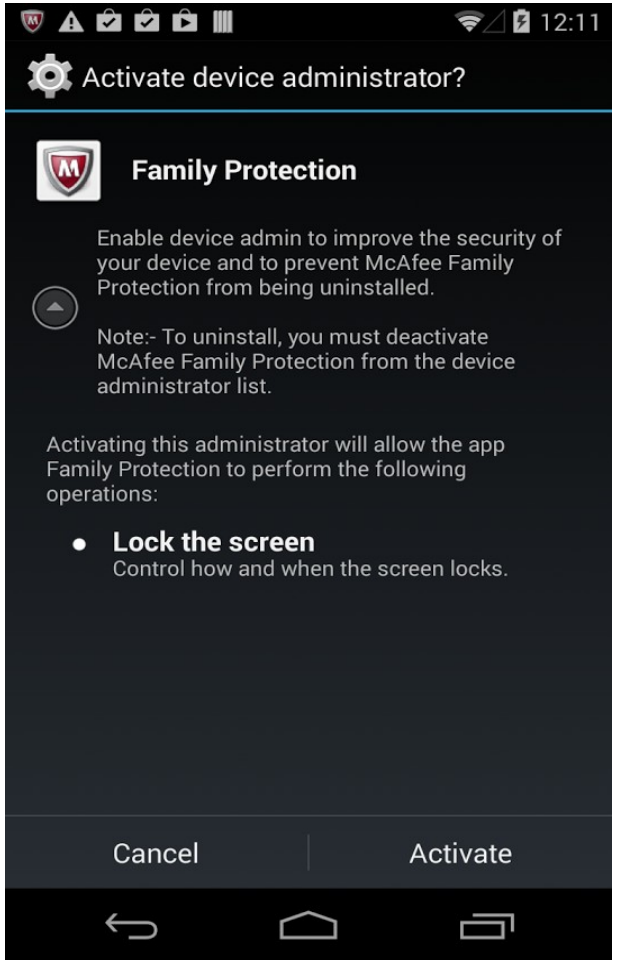


K9 Web Protection Browser (Android/Ios) sviluppata da Blue Coat (società leader nel campo del content filtering per le aziende), è la derivazione mobile del celebre browser per PC.



L'app Ignore No More (Android) per genitori apprensivi: se i figli non rispondono alle telefonate e agli SMS di mamma e papà, il cellulare si blocca (con password), permettendo solo chiamate ai genitori e quelle di emergenza

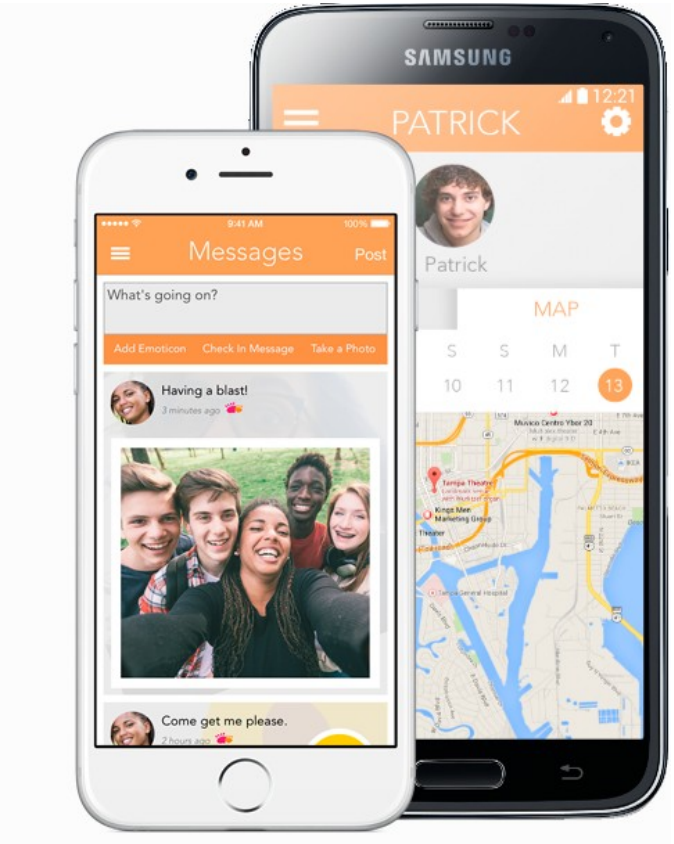
Cosa possiamo fare?



McAfee Family Protection

Questa app, a non si basa solo un browser, ma funziona con tutti. In tal modo, se anche il ragazzo installasse un altro browser, i contenuti verrebbero controllati allo stesso modo. L'app usa dei filtri divisi per categorie, quali "sesso", "gioco d'azzardo" e "droga", comunque personalizzabili.

Cosa possiamo fare?



MamaBear (sia per iOS che Android) permette un controllo pressoché totale delle attività svolte sul cellulare. Per i bambini ha una funzione di check-in veloce: una emoticon permette di conoscerne al volo la posizione. Ha anche un sistema per mandare con un clic un messaggio veloce al genitore: "Vieni a prendermi?".

Ottima la parte dedicata ai genitori. La app permette di:

- avere un report completo delle foto pubblicate su Instagram e dei post su Twitter, oltre a mostrare la lista dei nuovi amici e followers su entrambi i social network;
- ricevere notifiche su eventi definiti: l'aggiunta di un nuovo contatto, l'uso di termini inseriti in una sorta di "black list", il caricamento di una foto sui social o eventuali tag;
- controllare in tempo reale dove si trova il bambino e i posti dove è stato in precedenza;
- configurare la notifica di partenza e arrivo per particolari posti (per esempio la scuola).

Cosa possiamo fare?

My Mobile Watchdog

Questa app permette di tener traccia di tutto quello che viene fatto dal cellulare dei bambini. Consente al genitore, per esempio, di leggere i messaggi di testo inviati e ricevuti, vedere le foto scattate, bloccare le applicazioni, filtrare la navigazione così come impostare fasce di utilizzo e limiti di tempo.

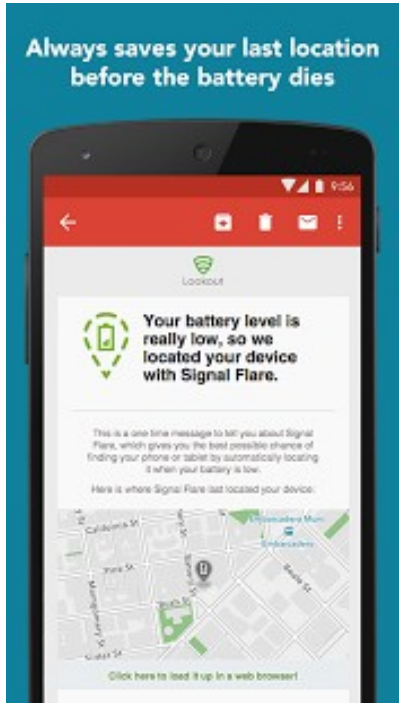
Le configurazioni si possono fare via SMS e il controllo delle attività avviene via Web. Non è uno spyware: la presenza del software sul telefonino è palese.

Cosa possiamo fare?

Per quanto riguarda Android vale la pena citare Lockout:

Antivirus, antifurto e localizzatore di dispositivi in un unico software

Lockout Security & Antivirus offre ai dispositivi la protezione essenziale da malware, virus, smarrimento e furto.



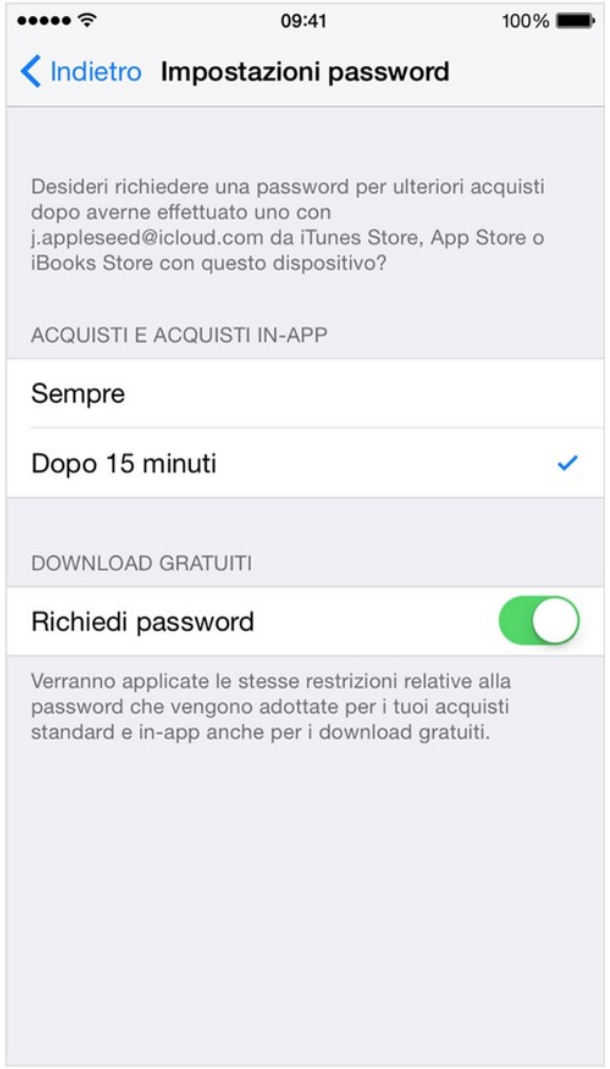
Acquisti in App

Gran parte degli sviluppatori li rendono disponibili gratuitamente sugli store così sono APPETIBILI.

- All'interno delle app è possibile fare acquisti per aggiungere componenti aggiuntivi, sbloccare livelli etc.
- Spesso le app dei giochi rendono impossibile vincere a chi non paga

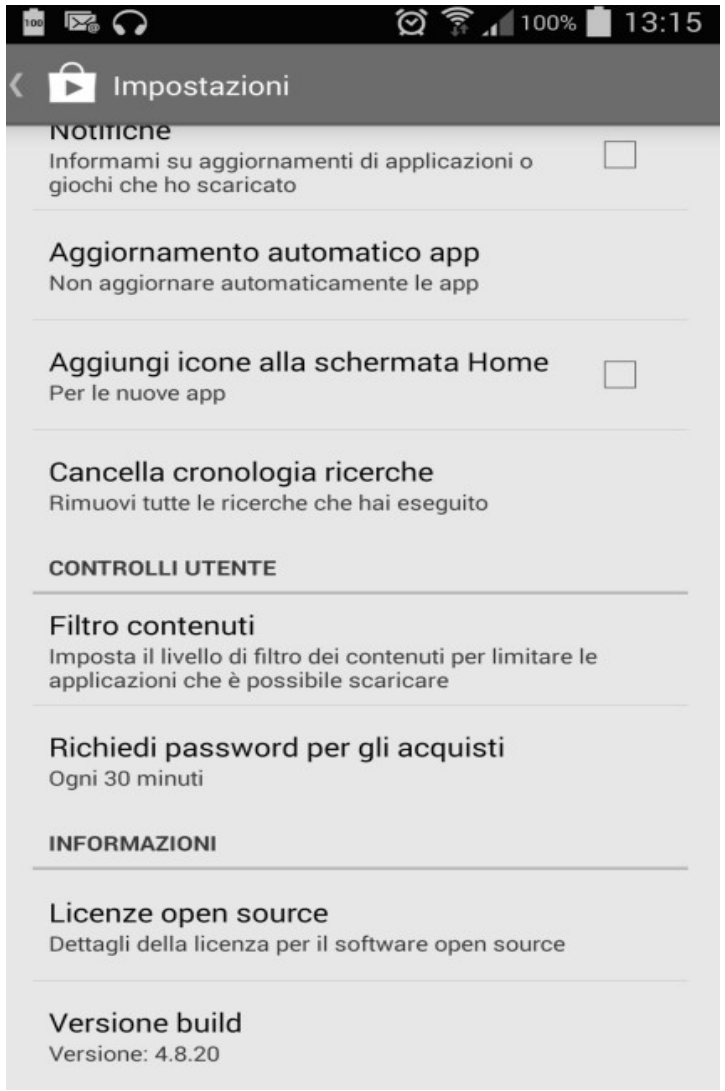
I casi di acquisti compulsivi con conti con parecchi zeri sono ormai moltissimi: citiamo quello più eclatante, avvenuto in Inghilterra, dove un bimbo è riuscito a spendere circa 2000 dollari in soli dieci minuti con un iPhone. (Soldi poi restituiti da Apple)

Cosa possiamo fare?



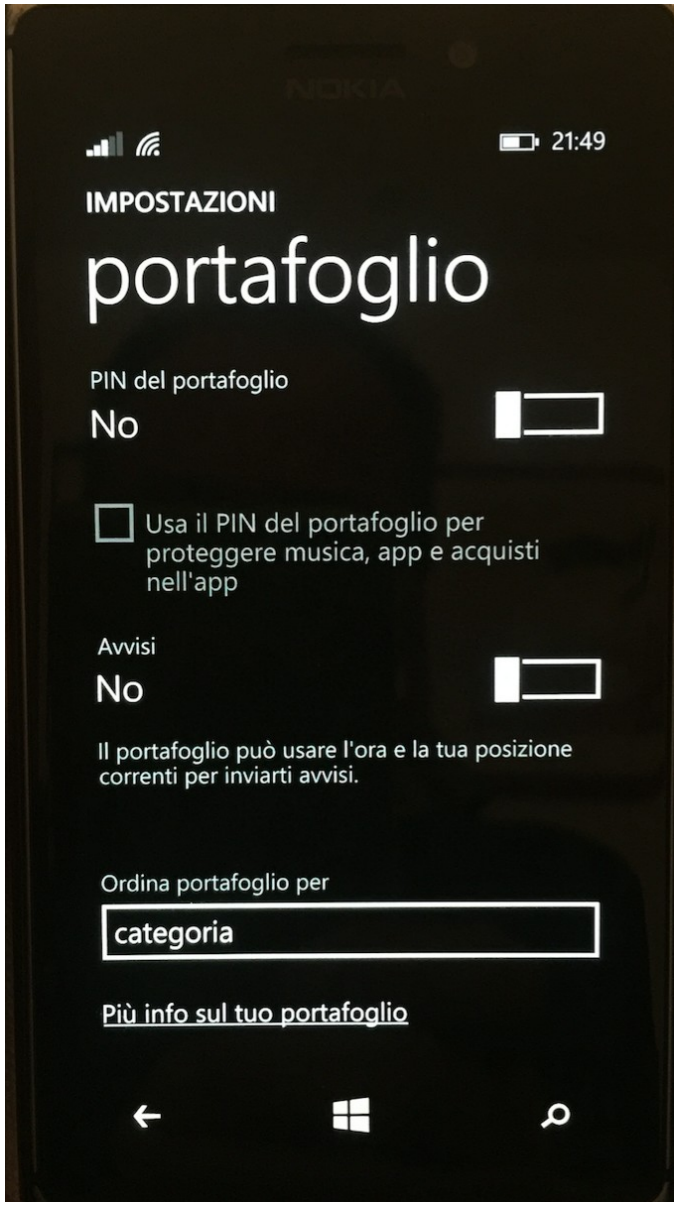
Su iOS se non avete attivato il touch-id per abilitare le impostazioni e restrizioni password dovete andare sotto impostazioni->iTunes Store e App Store -> impostazione password

Cosa possiamo fare?



Su Android l'impostazione è all'interno dello store. Basta andare nel Play Store e scegliere Impostazioni. Spuntare su "Usa la password per limitare gli acquisti". In questo modo solo chi ha la password dell'account Google può fare acquisti. Sempre in Impostazioni è possibile attivare un filtro contenuti per limitare la possibilità di scaricare applicazioni in base a criteri quali l'età.

Cosa possiamo fare?



Windows Phone 8

Infine parliamo di Windows Phone. Anche in questo caso per bloccare gli acquisti in-app su Windows Phone occorre agire sulla configurazione dello store delle app. Andate nelle impostazioni del Windows Store e fate tap sul pulsante PIN (che apre le impostazioni del portafoglio) e abilitate il Wallet PIN, che deve essere attivi (On). Da questo momento sarà chiesto il codice PIN, da inserire poi per ogni acquisto.

Grazie per l'attenzione

Se volete rileggere e approfondire il mio libro "SMARTPHONE SICURO" scritto con Gialuigi Bonanomi è disponibile sui maggiori siti di e-commerce.

Pubblico aggiornamenti di security regolarmente su Twitter @ donbrewerone

Se avete ulteriori domande domenico@imartinit.it