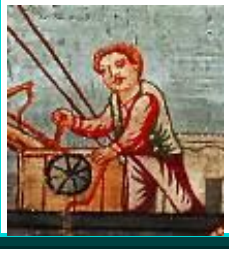

Appunti di viaggio **450**

Il Grande Fratello è già qui

1 dicembre 2017

Vietati gli smartwatch per bambini, *Redazione Scuola, 20 novembre 2017*

Germania

I genitori li usano per spiare i prof. L'autorità tedesca per le telecomunicazioni ha anche ordinato alle famiglie che li posseggono di distruggerli. «Orologi usati come cimici per ascoltare le lezioni in classe»

L'autorità tedesca per le telecomunicazioni ha vietato la vendita di smartwatch con funzioni di ascolto a distanza. Il presidente dell'authority Jochen Homann ha spiegato che, attraverso una app apposita, i genitori possono usare questi dispositivi elettronici per ascoltare di nascosto quello che succede attorno al bambino, un po' come succede con i monitor domestici che vengono venduti per controllare a distanza i neonati ma spesso vengono usati come «cimici» per spiare baby-sitter e tate. Solo che nel caso degli orologi le intrusioni dei genitori sono possibili anche fuori dalle mura domestiche.

Gran Bretagna

Una volta messi al polso di un bimbo di età variabile fra i 5 e i 12 anni, questi dispositivi possono varcare i cancelli della scuola e entrare in classe senza che nessuno li controlli, come viene fatto invece con gli smartphone. «Secondo una nostra ricerca - ha detto Homann - gli orologi vengono usati anche per ascoltare gli insegnanti mentre fanno lezione in classe». Ed è proprio in quanto potenzialmente capaci di violare la privacy di chi sta accanto al bambino, che l'autorità per le telecomunicazioni tedesca ne ha vietato la vendita e ha chiesto ai genitori di distruggere i dispositivi eventualmente in loro possesso.

Norvegia

Originariamente pensati per consentire di tracciare gli spostamenti dei bambini tramite Gps e di comunicare con loro tramite una carta Sim con funzioni molto limitate, questi dispositivi non solo si prestano a intrusioni indebite da parte di mamma e papà ma, come denunciato il mese scorso dall'associazione dei consumatori norvegesi, in realtà potrebbero esporre i più piccoli a rischi inutili. In altre parole, facendo leva sulle ansie e sul desiderio di controllo dei genitori, potrebbero trasformarsi in un'esca per malintenzionati e pedofili che, usando tecniche di hackeraggio elementari, potrebbero servirsene per localizzare le loro potenziali vittime o per sviare il Gps facendo apparire il bimbo in un posto diverso da quello in cui si trova.

La bambola, l'aspirapolvere, la tv «intelligente»

«Dal prossimo maggio le aziende tenute per legge a tutelare la privacy»

Il problema è la pigrizia. La nostra: chi ha la pazienza di leggere le cosiddette privacy policy dei prodotti che ci mettiamo in casa? Non lo facciamo. Ma dovremmo. Ce ne

pentiremo in futuro? Forse, probabile. Il risultato è che gli oggetti ci spiano. Ma non come faceva l'occhio del Grande fratello di orwelliana memoria: peggio. Ci mappano l'appartamento mettendo il risultato nel cloud, cioè le nuvole di dati sulla Rete. Ci riconoscono. Ci registrano, ci ascoltano, ci studiano.

Siamo sotto gli occhi (e le orecchie) di tanti Piccoli fratelli cui diamo le chiavi di casa. Come la famosa bambola Cayla che le autorità tedesche avevano vietato lo scorso anno perché era facilmente hackerabile e poteva essere usata per spiare i nostri figli. Le authority avevano esagerato? Se qualcuno si era posto la domanda ecco la risposta: no. E viene ora dal Garante della Privacy che ha messo sotto esame alcune categorie di prodotti già acquistabili in Italia, dunque in circolazione, che sono da considerarsi potenziali cavalli di Troia con cui i malintenzionati possono facilmente acquisire informazioni vitali sulla nostra quotidianità.

Parliamo di giocattoli: a partire da Cayla, ci sono una serie di prodotti poco innocenti con cui degli esterni possono entrare in contatto con i nostri figli. Aspirapolveri: di recente la società iRobot che produce Roomba, che mappa la casa e interagisce con l'assistente casalingo di Amazon, Echo, ha detto che i dati potrebbero essere condivisi con altre aziende, previo consenso. Un altro esempio di aspirapolvere che spia è il Botvac D7. Tv intelligenti: alcuni modelli registrano le nostre voci con le impostazioni di default. In pochi sanno come intervenire per bloccarle. E per chi ha voglia di farsi venire l'ansia basterebbe prendersi la briga di leggere nel dettaglio. Nell'informativa aggiornata al febbraio 2017 di Samsung per l'Italia, si legge: «Si prega di notare che Samsung, con il consenso informato dell'utente, può, anche bloccando funzioni di registrazione dei nostri comportamenti, raccogliere informazioni sull'uso dello Smart tv per altri fini». Cos'è il consenso informato? Il lato debole della faccenda: spesso è quel clic con cui siamo abituati a non pensare al problema.

Ma il problema c'è: «La considerazione di base è che la consapevolezza dei nuovi modi di comunicare è già in ritardo in generale per le comunicazioni tra persone. Ma sugli oggetti che comunicano c'è una discreta anarchia e un'inconsapevolezza di utenti e istituzioni. Dobbiamo affrontare seriamente i problemi che sono impliciti nel fatto che gli oggetti comunicano tra loro. Dagli oggetti si può identificare l'utilizzatore. Le istituzioni oggi beneficiano di un nuovo ordinamento europeo che entrerà in vigore il 25 maggio e ci dà la possibilità di pretendere dalle aziende che lavorano nel settore dell'Internet delle cose la cosiddetta privacy by design. Vuol dire che chi produce e gestisce l'oggetto è responsabile di valutare l'impatto-privacy e se non lo fa correttamente è suscettibile di sanzioni dure. Questo non lo sanno le istituzioni né le aziende».

Con la nuova normativa europea si passerà dalle parole ai fatti. Dovremo essere avvertiti se le informazioni che ci riguardano sono state rubate. Ma l'esperienza insegna che far rispettare le leggi su questi servizi in Rete, capillari e virali, non sarà facile. E ci sono ampie falle: le società che offrono comandi vocali fanno sapere che le nostre voci sono conservate nei loro server. Non c'è il diritto a farle cancellare quando revochiamo il consenso o cambiamo prodotto. Un diamante, diceva lo spot,

è per sempre. Forse lo sono anche le nostre impronte, i nostri volti e pensieri una volta concessi: persi, per sempre.

Svezia, contante quasi sparito, solo il 2% degli acquisti è pagato in cash

Nel paese scandinavo decine i bar, tabacchi e negozi accettano solo carte di credito. Risultato? Il contante sta "morendo in Svezia monete e banconote sono fuori moda. Il paese scandinavo, considerato tra i più virtuosi in Europa nel pagamento con carta di credito e bancomat, ha di fatto quasi abolito totalmente l'uso dei contanti e sono decine i negozi “free cash area”, esercizi nei quali è di fatto impossibile l'utilizzo della banconota.

Meno del 2% dei pagamenti avviene con la banconota locale. Negozi, ristoranti, tabaccherie, ma anche la bolletta della luce e il biglietto dell'autobus: gli svedesi pagano tutto in modo elettronico, basta un'applicazione nel telefono o una carta di credito. “In cinque anni gli svedesi hanno dimezzato gli acquisti fatti con la moneta locale". Il governo attribuisce l’estinzione della banconota all’alto livello tecnologico raggiunto dal paese, a una stagione dove i tassi d’interesse delle banche sono a vantaggio dei clienti perché vicino allo zero infine, alla fiducia che, contrariamente ad altri paesi europei, gli svedesi ripongono in questa tipologia di pagamento. Una preferenza accompagnata da numerosi benefici tra cui la lotta all’evasione fiscale e alla corruzione. Ma eliminare completamente la cartamoneta, obiettivo previsto nel 2025, sarà un’operazione difficile soprattutto se consideriamo le difficoltà dei pensionati nel gestire i pagamenti elettronici e i rendiconti online. Regno Unito, Canada, Usa e Giappone gli altri paesi che vanno verso la completa abolizione del denaro contante.

Droni con Wi-Fi per mappare l'interno di strutture chiuse

Tra il 2019 e il 2020 entrerà in vigore il regolamento unico europeo dei droni. Cade la distinzione tra aeromodelli e droni professionali e la patente sarà riservata a coloro che guidano un drone superiore ai due chili.

Uno dei maggiori freni alla diffusione di sensori sui droni era il consumo energetico, ma ora hanno messo a punto un sistema che usa il Wi-Fi, che consente di svolgere un sempre maggiore loro uso in nuovi campi ed ora in ambito catastale.

Ricercatori della University of California sono riusciti, facendoli lavorare in coppia a realizzare una mappa tridimensionale di una stanza senza finestre né altri "spiragli" dai quali poter spiare dimostrando che il Wi-Fi può essere utilizzato per mappare ambienti chiusi. Uno dei due droni è impegnato a emettere il segnale radio verso la struttura da analizzare, mentre l'altro si occupa di captare il segnale e inviare i dati raccolti a un centro di controllo esterno per una sorta di ecografia che consente di creare una mappa tridimensionale perfetta in ogni suo dettaglio e potranno anche essere utilizzati in caso di catastrofe per le operazioni di ricerca e recupero di feriti e sopravvissuti. La stessa tecnologia, potrà essere utilizzata in caso di rilievi archeologici per la realizzazione di opere che insistono in un'area dall'alto interesse storico. Da non sottovalutare, poi, i possibili utilizzi nel rilievo di eventuali crepe, fratture o

segni di cedimento in grandi strutture altrimenti difficilmente analizzabili.

Come fare a scoprire se il proprio cellulare è spiato.

Corrado Aaron Visaggio, 5 aprile 2016

Esistono molte app per spiare i cellulari. Perché? Spiare un cellulare non è una cosa bella, ma ci sono un sacco di persone che hanno motivi più o meno leciti per farlo: datori di lavoro che vogliono vedere cosa fanno i loro dipendenti durante le ore di lavoro o se hanno comportamenti non corretti nei confronti della propria azienda, genitori che vogliono monitorare i propri figli, persone che dubitano della fedeltà del partner e così via.

Cosa fa uno spyware? Raccoglie i dati del cellulare spiato, come i video, le foto, le mail, le registrazioni delle telefonate, le chat e gli sms che sono presenti sul cellulare spiato. Può attivare il gps, la videocamera o il microfono e diventare gli occhi e le orecchie dello spione nella vita privata della vittima. Uno scenario da incubo, ma molto più diffuso di quanto non s'immagini. La **buona notizia** è che per spiare un cellulare è necessario installare sul cellulare della vittima un'apposita app, ovvero lo spione deve comunque ottenere l'accesso al cellulare da spiare. La **cattiva notizia** è che non è che sia un'operazione così difficile da fare. Quindi, continua a valere la vecchia regola del "non accettare caramelle dagli sconosciuti!" Non fatevi regalare cellulari e comunque evitate di lasciarli nelle mani di qualcun altro. Mettete password complesse e cambiatele frequentemente e quando lasciate il vostro cellulare incustodito, anche per pochi minuti, anche in un ambiente amichevole e fidato, fate sempre in modo che sia bloccato con la password.

Non affidate mai il vostro smartphone a nessuno: lo spione può essere anche un amico, un collega o un parente, per cui la precauzione non è mai troppa. Considerate che le icone delle app possono essere nascoste, per cui il fatto che non compaiano icone di app sconosciute sul vostro display non vuol dire che l'app spyware non ci sia.

Fate attenzione perché anche voi potreste installarvi uno spyware sul cellulare inconsapevolmente: alcune app. Si tenga presente che uno spyware può fungere anche da "antifurto" sul proprio cellulare o per rintracciare il proprio apparecchio in caso di furto o smarrimento, quindi potrebbe essere utilizzato sul proprio cellulare anche come strumento di difesa. Con un'accortezza: tutte le informazioni sul cellulare spiato sono reperite su un sito web tramite credenziali, per cui se qualcuno ottiene quelle credenziali potrebbe, ovviamente, spiare il vostro smartphone.

Riconoscere che il proprio cellulare è spiato non è sempre facilissimo, ma ci sono alcuni suggerimenti che possono aiutarci a capire se c'è la possibilità che questo accada osservate se il cellulare: assume comportamenti strani, consuma troppo rapidamente la batteria, sentite rumori di fondo o interferenze, se ricevete strani messaggi di testo, se ha un traffico di dati esagerato.