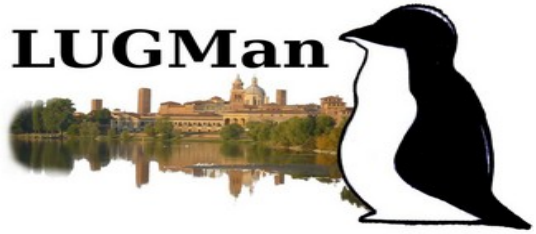


La tecnologia non è ne buona ne cattiva.

E' uno strumento come lo può essere l'automobile o il coltello.

Si tratta solo di conoscerla, di capirne i meccanismi e imparare ad usarla consapevolmente (e con prudenza).

I RISCHI: dal lato tecnico

VIRUS

Un virus è un insieme ridotto di istruzioni che si inserisce nei file presenti nel computer.
Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il file infetto, l'utente vede solo l'esecuzione del programma e non si accorge che il virus è ora operativo in memoria e sta compiendo le varie operazioni contenute nel suo codice.
Principalmente un virus esegue copie di sé stesso spargendo l'epidemia, poi svolge operazioni molto più dannose come cancellare, cifrare o corrompere file, far apparire messaggi, disegni o modificare l'aspetto del video, ...

I RISCHI: dal lato tecnico

ALTRI MALVARE

Un **trojan** o trojan horse (dall'inglese per **Cavallo di Troia**), è un tipo di malware che deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; installando il programma o aprendo un file, inconsapevolmente, si esegue anche il codice *trojan* nascosto. Spesso è diffuso con gli allegati delle mail.

Uno **spyware** è un tipo di software che ,senza farsi vedere, raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, etc...) senza il suo consenso, e li trasmette tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto.

Il **ransomware** è un malware la cui peculiarità è quella di introdursi in un sistema e bloccarne il funzionamento criptandone i dati. Poi avvine la richiesta di un riscatto (ransom) per poter ripristinare i dati, in caso contrario, i rischi sono due: che i dati vengano sottratti o rivenduti nel dark web.

I RISCHI: dal lato tecnico

IL PHISHING

Si tratta di una presa in giro dell'utilizzatore. Infatti ad essere attaccato non e' il sistema informatico in uso, quanto la psicologia (curiosita', insicurezza, ingenuita') dell'utente che viene ingannato e convinto ad agire in maniera sbagliata inviando a terzi informazioni "delicate" (password, codici di carta di credito, dettagli anagrafici).
Solitamente avviene con un messaggio di posta elettronica, apparentemente serio e ufficiale, inviato da agenzie e enti conosciuti (Poste, Banche, P.A., …), dove si comunica la necessità di cliccare su un link per comunicare dati o sbloccare una situazione. Non farlo, nessuno chiede mai dati in quel modo.
Può essere realizzato anche con SMS, e messaggi Whatsapp.
In questi casi l'unica protezione possibile è il sospetto e il "buon senso".

I RISCHI: dal lato tecnico

FURTO DI DATI

Di solito si tratta di credenziali di accesso a piattaforme (es.:home banking) in modo che poi qualcun altro le possa usare per vantaggio proprio.
Oltre ad utilizzare il phishing, viene anche usata la tecnica dello **sniffing**, cioè l'attività di intercettazione dei dati che transitano in una rete, solitamente il WiFi.
(Wikipedia)

Attenzione ai WiFi pubblici, e cambiare le password dei propri WiFi.

I RISCHI: lato sociale

- **Cyberbullismo**: forma di bullismo condotto attraverso strumenti telematici.. Rispetto al bullismo tradizionale, il cyberbullismo si realizza su internet sfruttando la Difficile reperibilità, l'indebolimento delle remore etiche, l'assenza di limiti spazio temporali.
- **Stalking**: atteggiamenti che affliggono un'altra persona, perseguitandola, generandole stati di paura e ansia.
- **Revenge porn** ("vendetta porno"): condivisione pubblica di immagini o video intimi tramite Internet, senza il consenso dei protagonisti.
- **Fake news**: creazione di disinformazione.
- **Cattura** e vendita dei nostri dati

FAKE NEWS = disinformazione

Consiste nella creazione di informazioni verosimili ma false.

La pericolosità sta nel fatto che possono orientare il pensiero della gente.

Si basa sul fatto che sul web, specie sui Social, chiunque (fonti attendibili e persone col proprio pensiero anche non argomentato) può pubblicare ciò che vuole.

Una campagna ben organizzata può fare danni irreversibili.

È fondamentale controllare la provenienza e la veridicità della notizia prima di divulgarla/condividerla (FACT CHECKING).

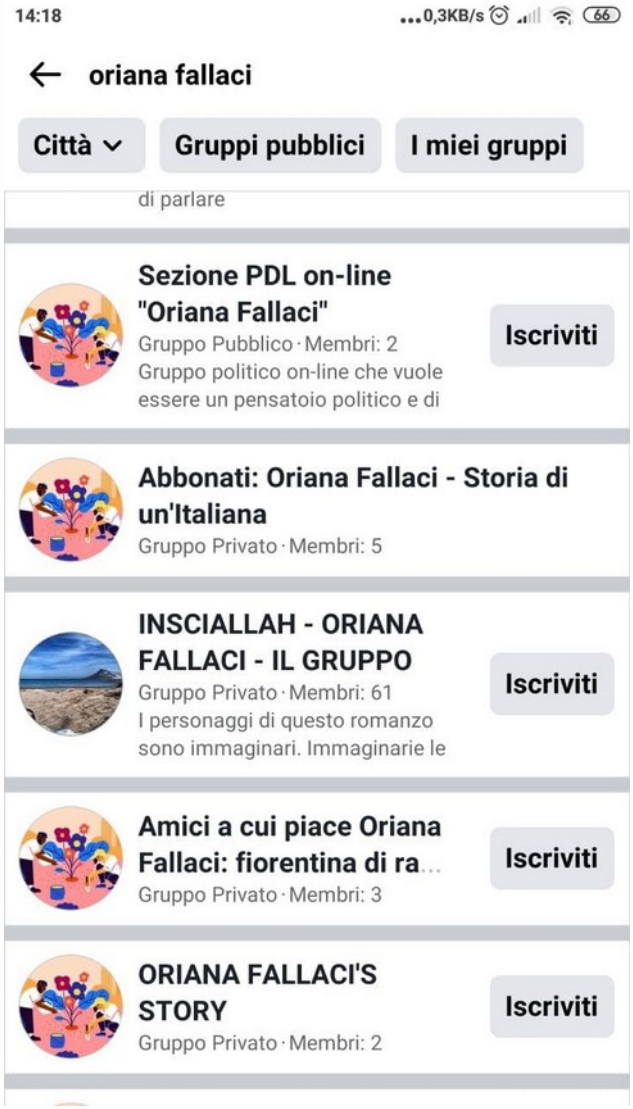
https://www.bufale.net

FAKE NEWS = disinformazione

Oriana Fallaci - Storia di un'Italiana
13 marzo alle ore 15:31 ·

Ficcatevi in testa una cosa: la Russia è un paese enorme, stracolmo di materie prime e minerali, in grado di assicurare ai suoi 150 milioni di cittadini sicurezza energetica e alimentare per secoli. Ha un debito netto pari a zero, enormi riserve auree, surplus commerciale e mercati di sbocco alternativi in forte crescita, popolati da più di un terzo della popolazione mondiale (Cina, India, Pakistan, Sud Africa, Brasile). É un paese con una identità fortissima, arte e cultura, abitato da un popolo forgiato nel ghiaccio che da agricolo e analfabeta in cinquant'anni è arrivato nello spazio. Ed è pure una superpotenza nucleare. Ma voi veramente pensate che un paese così fallisca dall'oggi al domani perché lo dicono i nostri "esperti", quelli del crollo di Wall Street e della Brexit che porterà le cavallette? Spegnete la tivù e iniziate a preoccuparvi di tutto ciò che non abbiamo noi. Che è un problema dannatamente più serio.

Apparsa su Facebook il 13 marzo 2022



I NOSTRI DATI: che ci fanno?

RACCOLTA: registrazione di quanti più dati possibili diretti o indiretti personali o tecnici (metadati).

ANALISI: con sistemi di Intelligenza Artificiale si incrociano tutti i dati raccolti in modo da poter produrre una ...

PROFILAZIONE: schedatura con interessi, orientamenti, abitudini, ecc… I profili, selezionati in base a criteri ben precisi sono molto appetibili a chi vuole convincere la gente.

PREDIZIONE: elaborando opportunamente i profili è possibile, in modo statistico, prevedere il comportamento di una certa categoria di profili circa un determinata situazione o tema o scelta.

ORIENTAMENTO: è possibile fare arriare a determinati gruppi di profili specifici messaggi, che possono orientare il pensiero degli stessi

I NOSTRI DATI: dove li raccolgono?

•Dallo **smartphone**: posizione, foto, video

•Dai **dispositivi smart** (assistenti vocali come Alexa, Google assistant, Siri, smart TV, smart watch, ecc…): ciò che sentono, fotografano, rilevano.

•Dalla **navigazione** che facciamo in Internet:
- coi traker: siti visitati, per quanto tempo, su cosa abbiamo cliccato;
- coi cookies: Strettamente necessari (per garantire il funzionamento), Miglioramento dell'esperienza, Misurazione (analisi del comportamento), Targeting e Pubblicità (rilevare gli interessi)

•Dai metadati delle **chat**: data e ora, posizione, identificativo del dispositivo, lunghezza del messaggio, flag di consegna, flag di lettura, ...

•Dai **post** e dalle **reazioni** (like) che pubblichiamo sui social: data e ora, posizione, identificativo del dispositivo, dati account, testo, immagini, like, condivisioni (con chi).

I NOSTRI DATI: perché li raccolgono?

La raccolta dei dati è continua ed alimenta enormi archivi.

Questi vengono incrociati con elaborazioni complicatissime svolte da programmi di intelligenza artificiale su computer potentissimi (e energivori), in modo da ottenere un profilo il più accurato possibile (**profilatura** = schedatura), in cui sono evidenziati informazioni personali (dati e foto), interessi, orientamenti, passioni, abitudini, qualsiasi informazione sia stato possibile recuperare.

I dati così (ben) organizzati vengono venduti, selezionandoli in base a criteri precisi, ad aziende o organizzazioni che intendono raggiungere un certo target con le proprie proposte commerciali o di altro genere.

Chi acquista questi dati è disposto a spendere parecchio perché sa che raggiungerà persone sensibili a ciò che gli viene offerto (comunque i costi sono sempre inferiori a quelli di una campagna pubblicitaria tradizionale)

I NOSTRI DATI: chi attua questa pratica?

I nomi più di rilievo sono:

Google (Mountain View): Gmail, Drive, Classroom, Meet, Youtube, Android, ….

Apple (Cupertino): iOS (sistema operativo dei cellulari Apple)

Facebook / Meta (Menlo Park): Facebook, Whatsapp, Instagram, ...

Amazon (Seattle): Amazon Web Services, Alexa Internet, Twitch.tv (A9.com, IMDb, Goodreads)

Microsoft (Redmond): Windows, Office 365, Teams, …

Comunemente indicati con l'acronimo **GAFAM**

ESEMPIO 1

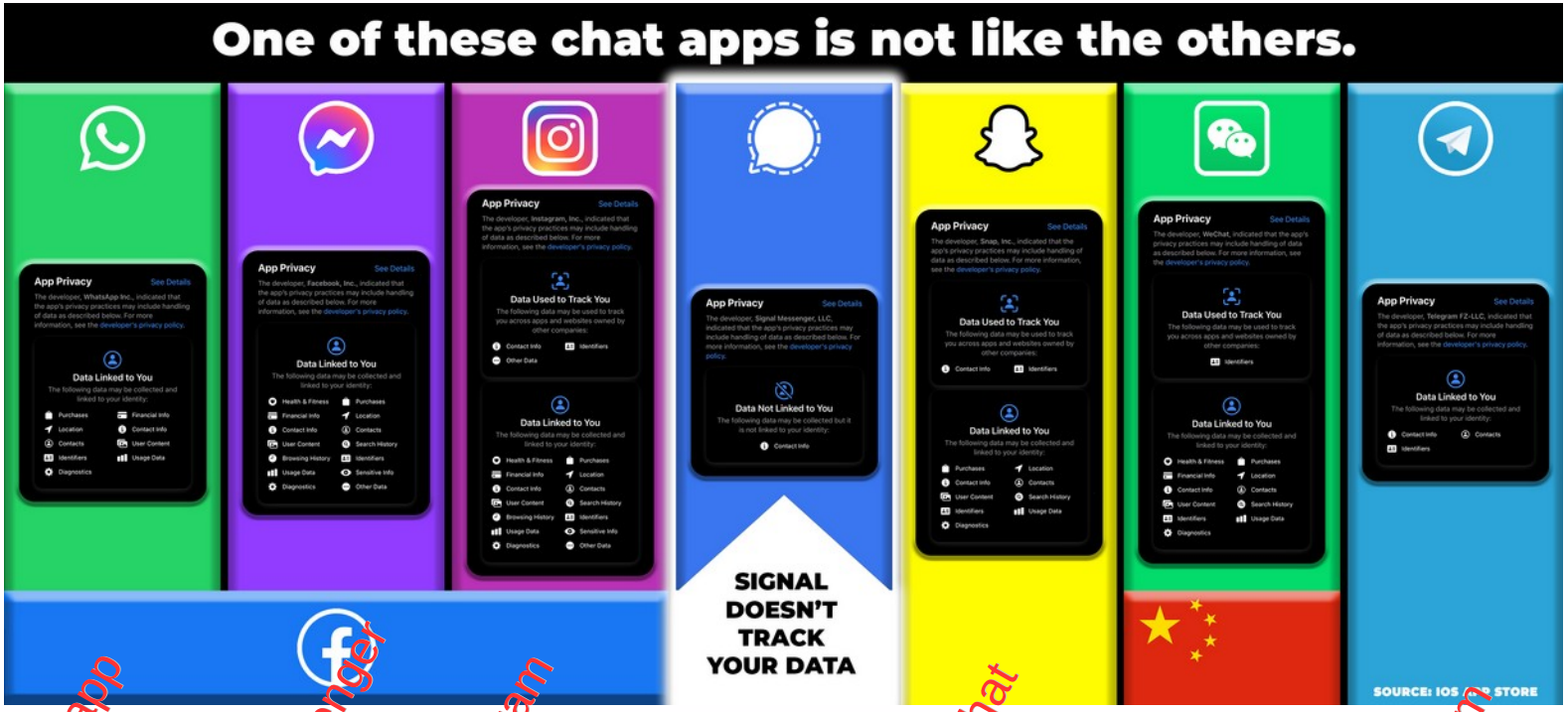
La raccolta di dati dai dispositivi viene solitamente motivata col “miglioramento della esperienza d’uso”, infatti essi comunicano tra di loro, anticipano le nostre richieste, BELLO! Ma già questo sta a significare che conoscono qualcosa di noi e quelle informazioni non sono nei dispositivi stessi (es.: Alexa comunica ad Amazon tutto ciò che sente, i nostri contatti, tutti i comandi che le diamo, quindi le nostre abitudini).

Ad esempio Google conserva:

- Cose cercate
- Siti web visitati
- Video guardati
- Annunci cliccati
- La posizione
- Informazioni sul dispositivo
- Dati relativi a cookie e indirizzo IP
- Email inviate e ricevute su Gmail
- Contatti aggiunti
- Eventi del calendario
- Foto e video caricati
- Documenti, Fogli e Presentazioni su Drive
- Nome
- Indirizzo email e password
- Data di nascita
- Sesso
- Numero di telefono
- Paese

ESEMPIO 2

Le informazioni raccolte da alcune App di chat, gli diamo il permesso accettando le CONDIZIONI D'USO.



DIPENDENZE

- **Dipendenza dallo smartphone**: è normale averlo sempre con se, lo si usa anche per attività per cui non è necessario, vengono proposti sempre più “utilizzi”, anche non necessari, pur che diventi sempre più insostituibile.
- **Dipendenza dai Social** (più diffuso tra i giovani): necessità di esserci pubblicando qualcosa o eprimendo reazioni (like, follower, visualizzazioni, …). È esattamente ciò che vogliono i Social: tenere agganciate le persone quanto più tempo possibile.
- **Incapacità di affrontare problemi** e di ipotizzare soluzioni perchè abituati a cercare soluzioni e risposte Internet o con l’uso di strumenti digitali. Le proposte che ci sono sono talmente numerose che non lasciano spazio alla creatività di ognuno (atrofizzazione).

DIPENDENZE

Dipendenza dall'uso di soluzioni digitali (lock-in):

- mi adatto ad usare una soluzione (software, piattaforma, …) magari proposto (o imposto) da altri,
- non mi preoccupo di verificare se c'è qualcosa di alternativo, più adatto, più etico, che limiti meno a mia libertà,
- lo uso per fare tutte le mie attività anche se non è l'ideale,
- obbligo i miei interlocutori digitali ad utilizzare la mia stessa soluzione per poter interagire con me diventando così parte del meccanismo.

(Le multinazionali dell'informatica da tempo fanno molto affidamento su questo fenomeno tant'è vero che fanno offerte non rifiutabili a scuole, associazioni, ministeri. È lo stesso metodo dei pusher)

CONDIZIONAMENTI

I social commerciali (FB, Instagram, YouTube, ecc…) hanno bisogno di registrare una quantità notevole di nostre informazioni (cosa leggiamo o osserviamo, i Like, le amicizie, …), e di proporci informazioni (pubblicità, notizie vere o false, ecc...).

Per raggiungere questi obiettivi devono tenere l'utente quanto più possibile connesso, ci riescono utilizzando algoritmi che presentano contenuti che attraggono o oscurano quelli che allontanano tra situazioni sensazionali, sport, situazioni divertenti - contenuti di violenza, sesso, odio - contenuti che interessano l'utente in base alla loro profilazione.

Quest'ultimo meccanismo è **pericoloso** perché si viene paralizzati in una bolla di informazioni, sono chiamate "filter-bubble" (bolla generata dai filtri) e/o "knowledge bubbles" (bolla di conoscenza).
Conseguenza di ciò è che di ogni situazione o argomento si osserverà solo l'aspetto che ci interessa/piace e non si viene a conoscenza della totalità delle informazioni (tra le quali si sono anche quelle contrastanti).
Questo spiega le estremizzazioni dei pensieri e dei comportamenti di certi gruppi di persone, e il meccanismo che può portare a orientare opinioni e scelte della gente.

Domanda:
Chi controlla il controllore, cioè colui che crea l'algoritmo che decide cosa far vedere?

SUPPONENZA

Essere convinti di possedere (conoscere / saper usare) la tecnologia.

Questo produce una disinvoltura pericolosa quando si utilizza il digitale (“ma si provo tanto non succede nulla”)

È un atteggiamento indotto dall’ambiente dell’elettronica di consumo (“è facile da usare, alla portata di chiunque, che rischio c’è?”)

Sento dire spesso dai tecnici informatici:
“Il pericolo maggiore sta tra il computer e la poltrona!”

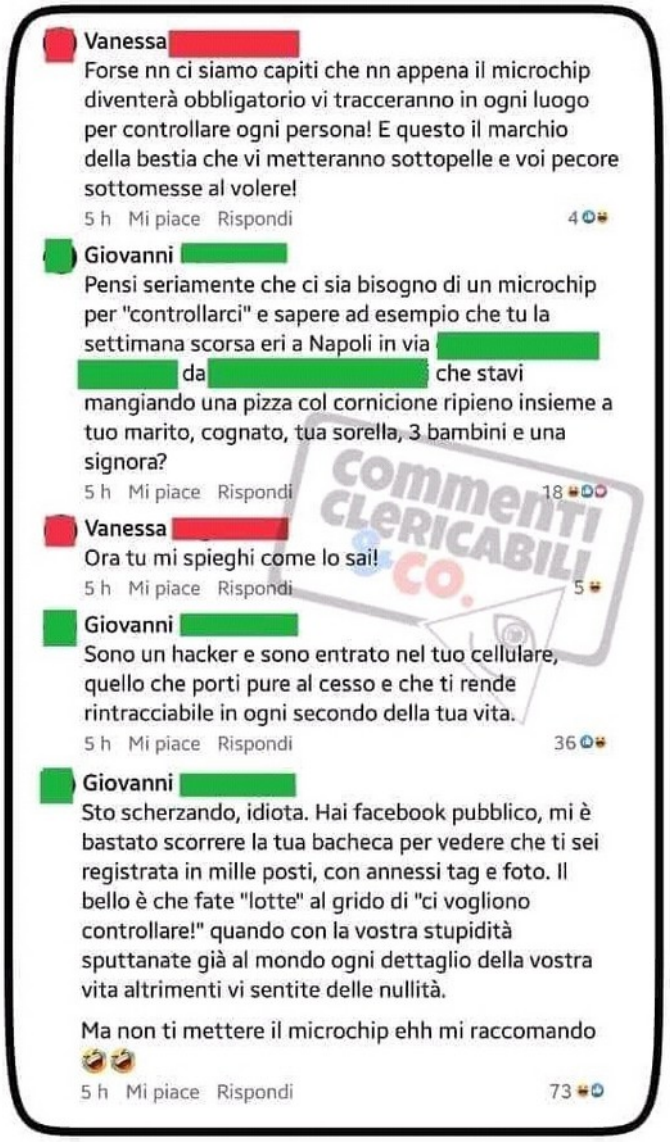
BUONE PRATICHE

- Essere sempre attenti e un po' sospettosi.
- Considerare gli strumenti digitali come STRUMENTI!
- Non lasciasci travolgere da realtà virtuali come i videogiochi devono restare solo divertimento.
- Chat, Social, blog:
  - non pubblicare informazioni personali (dati, foto, attività) e ridurre il numero dei destinatari con gli appositi filtri.
  - non lasciarci condizionare dai contenuti che vengono proposti.
  - verificare le notizie e le fonti prima di condividerle
  - mantenere uno spirito critico rispetto agli stili di vita che vengono proposti.
- Internet non dimentica nulla, attenzione a ciò che si scrive.

BUONE PRATICHE

Interessante CANDID CAMERA Belga

https://youtu.be/qYnmfBiomlo



COSA SONO?

ACCOUNT: identifica un utilizzatore di un sistema informatico con un nome utente e una password (sono dette credenziali). Cenni su accesso a 2 fattori.

HACKER: È un esperto di informatica e TLC (telecomunicazioni) che cerca di introdursi nei sistemi per capirne il funzionamento. Il temine è positivo ma solitamente è presentato dai media con una accezione negativa (pirata informatico). L'**HACKER ETICO** segnala agli amministratori le vulnerabilità rilevate.

CYBERSICUREZZA: identifica la resilienza, robustezza e reattività che un sistema informatico possiede per fronteggiare attacchi mirati a comprometterne il suo corretto funzionamento. Sono coinvolti elementi tecnici, organizzativi, giuridici e umani.

INFLUENCER: colui che pubblica costantemente sul web per avere quanti più follower possibili. Il pericolo sta nel fatto che i follower **spesso seguono in modo acritico i suoi consigli**.

Deep-web: Il web sommerso (o web profondo) è l'insieme delle risorse informative del World Wide Web non indicizzate dai normali motori di ricerca

Dark-web: Il web oscuro è il termine usato i contenuti del World Wide Web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software, configurazioni e accessi autorizzativi. Il dark web è una piccola parte del deep web.

https://it.wikipedia.org/wiki/Web_sommerso#/media/File:Deepweb_graphical_representation.svg