La Comunicazione - Note, Recensioni e Notizie n. 65

Anno 2022

Puoi fermarti prima di fare click?

Can you stop before click?

Agnese Scappini♦

Fabrizio Cirilli □

♦ Psicologa

□ PDCA Srl

Sommario

La tecnicizzazione dell'uomo: meccanicismo riduzionistico o intelligenza raffinata? Ma cosa significa quando lo strumento sembra (avere) il sopravvento sull'individuo? Attraverso una rivisitazione del nostro funzionamento basale, strutturale e cognitivo [1] comportamentale, osserviamo come e perché la tecnologia di oggi ci rende dipendenti e spesso vittime dei principali strumenti di comunicazione e lavoro; e come l'apprendimento diviene prima causa e poi paradigma indispensabile per padroneggiare lo strumento anziché soccombervi**.**

Abstract

The technicization of man: reductionist mechanism or refined intelligence? But what does it mean when the tool seems (to have) the upper hand over the individual? Through a review of our basal, structural and cognitive behavioral functioning, we observe how and why today's technology makes us dependent and often victims of the main communication and work tools; and how learning first becomes a cause and then an indispensable paradigm for mastering the tool rather than succumbing to it.

Keyword

Social engineering, Phishing

1 - Apprendimento

Partiamo da qui e facciamo alcune premesse: in prima istanza noi siamo esseri adattivi, ovvero cresciamo per apprendimento (adattamento), e siamo per questo plastici. Il nostro cervello è plastico, non è elastico, questo significa che dinanzi ad una modificazione subita (dall'esterno) o attuata (dall'interno, ad es. acquisizione nuova abitudine) tende a mantenere la nuova forma.

2 - Osserviamo, ora, cosa significa Apprendere?

È la capacità che abbiamo di acquisire nuove competenze, e lo facciamo per tutta la durata della nostra vita seppur con diverse disponibilità di risorse, è una straordinaria attitudine se pensiamo di essere l'unico animale quasi del tutto sprovvisto di istinti (al massimo siamo dotati di riflessi, primi e principali rivolti a creare attaccamento/socialità), nasciamo infatti (per via dell'assunzione della postura eretta e della riduzione del bacino della donna, in uno stadio precoce dello sviluppo tanto da renderci alla nascita e per un tempo ancora lungo successivo) non-autosufficienti. "L'altro", inteso nel senso più ampio, è il garante della nostra sopravvivenza non solo in virtù del nutrimento, ma anche e soprattutto della 'cura'. L'altro, diviene il modello da cui apprendiamo, poiché lo facciamo per imitazione.

Quindi, se ogni cosa che facciamo e che sappiamo fare l'abbiamo appresa, possiamo immaginare come noi apprendiamo continuamente. Pensiamo a quanto facilmente apprendiamo una nuova abitudine (il caffè dopo pranzo nel nuovo bar sotto casa), a come facilmente ci adattiamo al nuovo capo, al nuovo collega così via…

Ma qui introduciamo un'altra caratteristica fondamentale: l'apprendimento avviene attraverso i cosiddetti 'rinforzi' (positivi ma anche negativi), cioè una certa azione viene appresa se è seguita da una conferma, che sia un premio, un piacere; il premio per antonomasia è la risposta dell'altro: *riportando un bel voto il papà mi sorride fiero, prendendo un caffè al nuovo bar sotto casa incontro la ragazza che mi piace*; associo i due stimoli e

ripeterò l'azione l'indomani. Questo è infatti ciò che va ad attivare il famigerato sistema dopaminergico[1] o sistema della ricompensa (il meccanismo alla base delle dipendenze).

Ecco che ci inoltriamo nel pieno del nostro discorso, andiamo allora ancora oltre…

Fondamentale è sapere che contrariamente a quanto si è ritenuto fino al XVIII - XIX secolo, l'apprendimento è un processo *totalmente inconscio* [2] (tranne ovviamente nei casi in cui vogliamo deliberatamente imparare qualcosa). La maggior parte del tempo apprendiamo e lo facciamo in maniera inconsapevole e a seguito di rinforzi, che poi andiamo a riproporre, divenendo in parte dipendenti da quei comportamenti appresi.

Inizia a delinearsi una qualche sensazione riguardo la domanda in abstract: *come qualcosa può prendere il sopravvento su di noi*!

Noi apprendiamo costantemente e la nostra garanzia di sopravvivenza è 'l'altro', quindi tutti i comportamenti che creano connessione con l'altro o feedback dall'altro sono essenziali, diremmo esistenziali, per noi. Pensiamo ora a tutti i nostri strumenti di comunicazione che amplificano questa nostra competenza/esigenza primaria: la relazione, la connessione con l'altro. Possiamo aver idea di quanto ci piaccia il suono, il bip ad esempio, dell'arrivo di un messaggio (contatto) e di quanto lo stesso attivi il nostro sistema dopaminergico. Ci piace grazie alla dopamina che viene rilasciata[2], un messaggio che arriva è come un sorriso, un rinforzo quindi. Se tutto questo rimane, tuttavia, sotto la soglia della consapevolezza iniziamo anche a comprendere con quanta facilità un click diventi qualcosa di sempre più impellente e importante fintanto da non riuscire più a controllarlo; ecco che diventiamo vittime di quella mail o di quella notifica push il cui click può nascondere virus o altre truffe sul web.

[1]La dopamina è un ormone molto importante legato all'attaccamento e al bisogno. Stimoli che producono motivazione e ricompensa (fisiologici quali il sesso, cibo buono, acqua, o artificiali come sostanze stupefacenti, o elettrici ma anche l'ascolto della musica, in particolare alcuni tipi di suoni o timbri vocali), stimolano parallelamente il rilascio di dopamina.

[2]Già nel 2012 gli psicologi parlavano tranquillamente di "addiction" e di "disorder"

3 - Come difendersi?

Se siamo esseri in continuo apprendimento… apprendere è il segreto: investire sull'apprendimento di nuove competenze capaci di neutralizzare questi automatismi è il segreto.

4 - Cosa possiamo fare?

Una volta capito il meccanismo, dietro la nostra "clicchite compulsiva", dobbiamo solo imparare a non farci catturare dal vortice e darci il tempo di capire chi ci scrive e cosa ci viene chiesto di fare.

Le tecniche di phishing, attraverso e-mail più o meno efficaci, mietono moltissime vittime sul web.

Dal dirottamento di e-mail di pagamento agli inviti romantici c'è un po' di tutto oramai. In alcuni casi ci vengono compromessi telefoni e/o computer, in altri ci vengono sottratti soldi o, peggio, diventiamo prede di reati ancora più subdoli e violenti. Il ritmo frenetico della nostra vita e la diffusione sempre più capillare dei mezzi social sono un terreno fertile per sviluppare queste tecniche, sfruttando i meccanismi del nostro cervello che abbiamo visto nei paragrafi precedenti

5 - Come possiamo difenderci?

Potremmo dire che la giusta risposta passa per i seguenti punti:

1. Evitare di aprire messaggi ed email "non attese" o sconosciute, almeno fin quando non siamo seduti tranquillamente o possiamo concentrarci sul testo; ad esempio le rapide risposte mentre siamo alla guida, o mentre siamo impegnati in altre cose, favoriscono il comportamento indotto e non quello riflessivo-razionale. Quante volte avete risposto di getto per poi pentirvi un istante dopo? Quante volte avete mandato una risposta automatica inviando informazioni e dati a chi non avreste voluto? Il tempo gioca un ruolo decisivo in questi casi, sia nella risposta sia nelle conseguenze. Diamoci quindi il tempo di analizzare, capire e decidere. La fretta non gioca mai un ruolo positivo in questi casi.

2. Verificare che il mittente sia effettivamente una persona a noi nota o che sia chi dice di essere; spesso le e-mail ed i messaggi trappola provengono da destinatari ignoti o indirizzi simili ma non identici, ad esempio un account reale del tipo **cirillif@xxx.yy** può essere facilmente rielaborato in **cirilllif@xxx.yy**: veramente difficile, rispondendo di getto, notare la "l" di troppo aggiunta nel mezzo. Se il messaggio arriva da un numero o da un account sconosciuto è opportuno verificare su internet se quel nome, numero o account e-mail non sia presente già in qualche forum o in altre casistiche già pubblicate. In questi casi è buona regola verificare che la e-mail arrivi veramente dal mittente, magari basta una telefonata o una ricerca su internet per chiarire con chi abbiamo a che fare. Comunque, una verifica su un canale diverso e darsi il tempo di verificare sono strategie vincenti in caso di dubbi.
3. Spesso questi messaggi trappola hanno un link da "cliccare" per ottenere qualcosa; anche qui nella fretta non riusciamo a fare un controllo elementare: semplicemente passando con il mouse su quel link (senza cliccare!) il vero indirizzo web compare da qualche parte sul vostro schermo, se i due indirizzi vi sono familiari o coincidono allora (forse) non è un link trappola. Ad esempio: se il messaggio proviene dal corriere XYZ, che vi invita a cliccare su un link per vedere il perché del ritardo nella consegna, la cosa più semplice è verificare che quello che compare nel vostro schermo sia il vero sito di XYZ e non un groviglio di lettere e numeri incomprensibili. Ultimamente vanno molto le chiamate telefoniche o SMS provenienti dalla "vostra" banca per avvisarvi che c'è un addebito rilevante sul vostro conto e che questo è stato bloccato per ragioni di sicurezza, subito dopo arriva l'immancabile richiesta di credenziali che l'operatore (gentilissimo) si propone di modificare o verificare per voi…

4. Leggete con attenzione il testo; e-mail e messaggi possono essere generati da traduttori automatici in varie lingue, partendo da un messaggio originale, oppure possono essere scritti da persone che non padroneggiano la lingua. Questi fattori concorrono a generare testi "sgrammaticati" che ci aiutano a capire che qualcosa non va. Se il nostro campanellino interno o la nostra vocina interna ci dicono che qualcosa non va è probabile che sia vero. L'istinto cerca di avvisarci, sta a noi dargli ascolto. Anche qui valgono le regole viste nei punti precedenti.

6 - Tutto ciò è sufficiente?

Certamente mette le basi per una maggior consapevolezza del problema ma non necessariamente è sufficiente a toglierci l'abitudine o controbattere tutti i tipi di potenziali attacchi cui potremmo essere soggetti. Del resto, i crimini informatici hanno raggiunto una complessità e una dimensione così vasta da essere scarsamente gestibili al 100%, per chiunque.

La consapevolezza è un punto fondamentale ma soprattutto la capacità di "investire sull'apprendimento di nuove competenze, capaci di neutralizzare questi automatismi, è il segreto".

Essere consapevoli è il primo passo: 'ora so che c'è un pericolo!'. Come affrontarlo e gestirlo lo si impara acquisendo nuove competenze.

Nelle aziende, di tutte le dimensioni, si sviluppano campagne di awareness e programmi di formazione su questi temi. Investimenti rilevanti, per evitare di cadere nei tranelli e/o fornire involontariamente un punto di attacco ai malintenzionati.

ENISA[3] mette a disposizione una serie di video clip, illustrazioni, screen savers e poster[4] che potrebbero essere utilizzati per sviluppare il giusto grado di sensibilità a questi temi, che, con

[3] https://www.enisa.europa.eu

[4] https://www.enisa.europa.eu/media/multimedia/material

l'attuazione di poche e semplici contromisure, può fare la differenza sia nel lavoro sia nella vita privata.

Interessante l'attenzione di ENISA su questi temi per i bambini e per le famiglie: forse i punti più deboli del nostro attuale sistema di risposta, personale e professionale.

7 - Chiedere aiuto

Un ultimo punto deve essere trattato e considerato, in questo scenario: la richiesta di aiuto.

Nell'attuale società pare che chiedere aiuto sia segno di debolezza, di dipendenza, di fallimento. In questi casi è invece quasi un obbligo. Nessuno di noi può avere la certezza assoluta di ciò che sta accadendo, né tutte le competenze necessarie per gestire questo tipo di attacchi.

È fondamentale sapere che si può e si deve chiedere aiuto, in caso di dubbi e/o in caso di non conoscenza delle situazioni.

In caso di attacco informatico, le aziende dispongono di particolari presidi (i cosiddetti Security Operation Center – SOC – e gli Incident Response Team - IRT), formati da specialisti in grado di analizzare e comprendere cosa sta accadendo, decidendo la miglior risposta. Tipicamente sono gruppi di persone con competenze miste, in grado di mettere a fattor comune le loro esperienza e conoscenza delle tematiche e trovare la risposta più efficace a fronte di un attacco.

Quando questo non basta abbiamo i CERT (Computer Emergency Response Team), anche a livello di nazione (CSIRT[5]), che si occupano di gestire e coordinare le azioni in caso di attacchi su larga scala.

Quindi chiedere aiuto non è un fatto negativo ma una possibilità che ci viene data nel mondo del lavoro.

[5] https://csirt.gov.it

Nel mio privato a chi mi rivolgo? In caso di dubbi o problemi una possibilità è rivolgersi alla Polizia Postale[6], il cui sito è ricco di informazioni, oltre che fornire un punto di contatto in caso di necessità.

8 - Conclusioni

Pensare prima di cliccare è qualcosa che dobbiamo imparare a fare, disinnescando gli automatismi e salvaguardando la nostra vita e i nostri interessi.

Per imparare abbiamo svariate opzioni, dall'applicazione di piccole semplici regole fino al supporto delle istituzioni e delle forze di polizia.

Sta solo a noi decidere di cambiare e non rispondere più come un automa a quel subdolo "bip" che ci rende schiavi di una risposta immediata e impulsiva.

9 - Bibliografia

[1] Carr, A., "Internet ci rende stupidi? Come la rete sta cambiando il nostro cervello", 2010

[2] Jaynes, J, "Il crollo della mente bicamerale e l'origine della coscienza", 1984

[6] http://www.commissariatodips.it