LUIGI GOBBI

Nella mente dell'hacker

Tecniche di persuasione e manipolazione mentale in rete

illustrazioni di Milian Zheng
prefazione di Giovanni Ziccardi

SAGGI

a Lisa

Indice

Prefazione

In un'era digitale in così rapida evoluzione, la tecnologia attorno a noi continua a trasformare il modo in cui interagiamo con gli altri, comunichiamo e conduciamo i nostri affari.

Mentre il confine tra il mondo fisico e quello digitale si confonde sempre di più, la società si trova sull'orlo di un profondo cambiamento di paradigma, non solo sociale ma anche giuridico, accompagnato da opportunità senza precedenti e, soprattutto, da profonde vulnerabilità.

L'aumento pervasivo dei crimini informatici in questi ultimi cinque anni rappresenta una sfida che si riverbera nel mondo accademico, nell'industria, nel governo e nella vita dei cittadini di tutti i giorni.

La necessità, sempre più percepita, di sicurezza informatica ha superato i confini tradizionali e si estende ora a ogni aspetto della vita connessa delle persone.

Il primo merito di questo libro è, allora, sicuramente un'esplorazione rigorosa ma, al contempo, assai vivace e piacevole per il lettore di alcuni aspetti essenziali correlati alle cosiddette "minacce digitali", alle loro conseguenze e al ruolo indispensabile della sicurezza informatica, in particolare per la "gente comune" e l'utente non professionista.

Il ruolo degli hacker, quelli veri, nella rivoluzione digitale è noto, e apprezzato, da tempo. Il libro affronta anche, però, le situazioni patologiche, cercando di far comprendere come una comodità senza precedenti fornita dai servizi online, e una connettività globale, possano anche generare una serie di minacce, e sfide, che non possono essere trascurate né passate sotto silenzio.

Le pagine di questo libro descrivono un panorama digitale che può essere obiettivamente complesso da comprendere per il cittadino comune, tanto da diventare terreno fertile per attori malintenzionati e criminali informatici che sfruttano le vulnerabilità a fini di guadagno personale o per "semplice" disturbo. Al contempo, però, l'autore vuole far comprendere come non si stia più parlando di un evento raro, o accademico, o da confinare nell'ambito delle sottoculture: è un fenomeno che ha permeato il tessuto stesso dell'esistenza moderna, causando non poco disordine, e che, pertanto, riguarda tutti.

Purtroppo, i crimini informatici, con le loro molteplici manifestazioni, richiedono un attento esame per comprendere appieno la portata del problema.

Nel libro, ad esempio, vengono giustamente evidenziati degli schemi fraudolenti che si accompagnano ad attacchi di phishing (spesso legati alla manipolazione dei comportamenti e delle emozioni delle vittime) e a terribili attacchi ransomware in grado di paralizzare le attività di interi enti e aziende.

Questo libro non solo descrive questo multiforme sottobosco criminale ma cerca di raggiungere un obiettivo più ambizioso: far comprendere come l'uomo sia, oggi, al centro di questi attacchi, che puntano non più ai sistemi informatici ma al cervello delle persone.

È molto più facile, del resto, passare dalla tastiera di un dipendente distratto che investire risorse e competenze per cercare di violare un sistema o una rete.

Il volume è ricco di casi reali. Del resto, il riflettere sulle disgrazie altrui – un po' come avviene nei grandi romanzi russi – è il modo migliore per evitare che certe vulnerabilità accadano sui nostri sistemi.

L'autore, professionista del settore, ci tiene, in tanti passaggi, a precisare come l'importanza fondamentale della sicurezza informatica si estenda, oggi, a tutti i settori della società, e non sia più una responsabilità esclusiva delle agenzie governative, delle aziende o dei professionisti informatici: è diventata una sorta di "responsabilità collettiva", condivisa dagli individui che devono adottare misure proattive per proteggere sé stessi e i propri beni digitali. Si pensi, a tal fine, all'importanza della sicurezza cosiddetta "organizzativa", fondamentale quanto quella tecnica.

Ci sembra che quest'opera, in conclusione, sia perfetta (anche) per riflettere sulla propria sicurezza personale e offra una guida completa per comprendere le complessità della tutela della propria vita digitale, della salvaguardia delle informazioni personali e della protezione dei propri beni online.

In particolare, in più parti del volume si ribadisce la necessità di educazione e consapevolezza: una società alfabetizzata in materia digitale diventa molto più sicura per navigare nel panorama sempre in evoluzione delle minacce. E da molte di queste pagine si possono ricavare ottime idee per lo sviluppo di politiche, linee guida etiche e iniziative educative, garantendo così, per tutti, un ecosistema digitale sicuro e resiliente.

Giovanni Ziccardi


CENTRAL INT ENCE AGENCY
UNITED STATES OF AMERICA

Capitolo 1

Ti possiedo

> I dilettanti hackerano i sistemi, i professionisti hackerano le persone.
>
> *Bruce Schneier*

Nell'immaginario collettivo l'hacker è spesso raffigurato come un misterioso soggetto incappucciato, con il volto coperto dalla ghignante maschera di Guy Fawkes, che si diverte a osservare decine di monitor nascosto in un bunker stracolmo di tecnologia avanzatissima.

Immaginate dunque lo stupore che devono aver provato gli ufficiali della polizia britannica che, nel febbraio del 2016, dopo aver fatto irruzione in una casa popolare appena fuori Leicester per arrestare quello che ai tempi era considerato uno dei più temibili hacker in circolazione, si ritrovarono ad ammanettare un pallido e smarrito adolescente in pigiama e pantofole.

Immaginate anche la reazione dell'ex direttore della CIA, John Brennan, e dell'ex vicedirettore dell'FBI, Mark Giuliano, quando appresero che era proprio quel ragazzino a celarsi dietro il fantomatico personaggio di Cracka, il leader del gruppo criminale Crackas With Attitude, che da mesi li teneva sotto scacco.

Il ragazzino in questione era Kane Gamble, uno studente di appena sedici anni affetto da una lieve forma di autismo, che ai tempi conduceva una vita apparentemente normalissima.

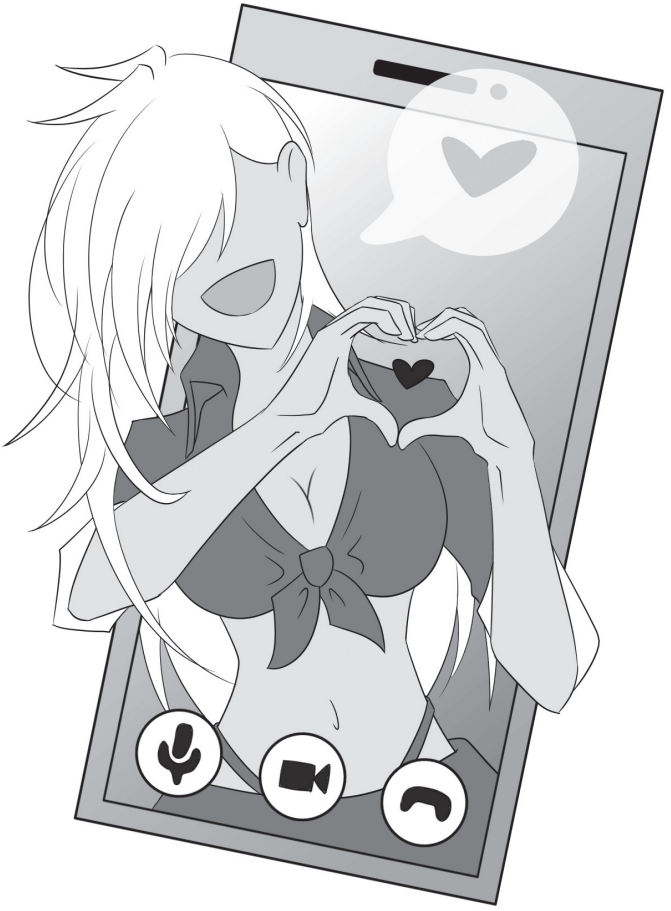
Capitolo 4

Sextortion

> Il modo migliore per imporre una idea agli altri è quello di far credere che provenga da loro.
>
> *Alphonse Daudet*

Ryan Last era un ragazzo di diciassette anni come tanti, con i suoi interessi, le sue passioni, i suoi sogni. Frequentava la scuola superiore di Morgan Hill, in California, a pochi chilometri dalla sua abitazione di San José, dove viveva con la sua famiglia. Nel tempo libero si divideva tra hobby e attività di svago, tra cui spiccavano le arti marziali, di cui vantava una cintura nera di secondo livello, ma soprattutto la passione per gli animali, che da sempre condivideva con suo fratello minore, assieme al quale, tra l'altro, aveva iniziato ad allevare un agnellino.

Il 4 marzo del 2022, al termine di una giornata come tante, Ryan cenò con la sua famiglia, chiacchierando del più e del meno e mostrandosi allegro come sempre. Verso le 22:00, come di consueto, diede quindi la buonanotte a tutti e andò a chiudersi in camera. Sua madre Pauline, in quel momento, non avrebbe mai potuto immaginare che quella sarebbe stata l'ultima volta che lo avrebbe visto vivo. Poche ore dopo, infatti, fu proprio lei a ritrovare il corpo senza vita di Ryan, disteso nel suo letto, con a fianco un'assurda lettera di addio.



Capitolo 5

Ordini dall'alto

> L'irriflessivo rispetto per l'autorità è il più grande nemico della verità.
>
> *Albert Einstein*

Una delle tecniche di ingegneria sociale in assoluto preferite dai *cybercriminali* moderni è quella di impersonare una figura autoritaria per poi avanzare delle richieste che, agli occhi delle vittime, potranno apparire come dei veri e propri ordini, da eseguire alla svelta e senza indugio. Si cerca di sfruttare, in questo caso, il principio emotivo dell'autorità, secondo il quale le persone sono maggiormente inclini ad assecondare le richieste provenienti da fonti autoritarie.

La storia di Kane Gamble, che appena sedicenne riuscì a impersonare l'allora direttore della CIA e a farsi consegnare le password dei suoi account privati, ne è un esempio evidente, ma ce ne sono tantissimi altri.

Prendiamo le *CEO scam*, che nel 2023 hanno generato proventi criminali per svariati miliardi di euro, superando persino gli introiti derivanti dai riscatti dei famigerati attacchi *ransomware*. Si tratta di una particolare tecnica di *phishing*, che consiste nell'impersonare il dirigente di un'azienda, tipicamente l'Amministratore Delegato – in inglese, appunto, il CEO – e contattare uno o più sottoposti di quest'ultimo, chiedendo di effettuare un pagamento urgente verso un conto bancario fittizio.

Capitolo 7

FOMO

La fretta genera l'errore in ogni cosa.
Erodoto

L'oro è da sempre considerato il materiale prezioso per eccellenza, simbolo di ricchezza, stabilità e potere.

Alle sue spalle c'è una storia millenaria, ricca di fascino e leggenda, che affonda le radici nella prosperità dell'antico Egitto e passando attraverso i fasti della Magna Grecia e dell'Impero romano arriva fino all'età contemporanea.

Il grande valore che da sempre gli viene attribuito è dovuto in parte alle sue eccezionali proprietà fisiche, come la duttilità e la malleabilità, che lo rendono particolarmente facile da lavorare, oppure la resistenza e l'incorruttibilità, che lo fanno adattare perfettamente, ad esempio, alla coniazione di monete.

C'è poi una componente estetica non trascurabile, riconducibile alla sua lucentezza e brillantezza, che gli conferisce un aspetto elegante, raffinato e quindi ideale per la realizzazione di gioielli, decorazioni e ornamenti.

Tuttavia, oltre alle suddette proprietà che potremmo definire intrinseche, c'è anche un'altra qualità che contribuisce a renderlo particolarmente prezioso, ovvero il fatto che si tratta di un bene raro, o per meglio dire "scarso".

L'oro, in effetti, è presente in natura solamente in quan-

tità limitate, peraltro concentrate in zone della terra isolate e difficilmente accessibili, il che rende il suo processo estrattivo complesso e oneroso.

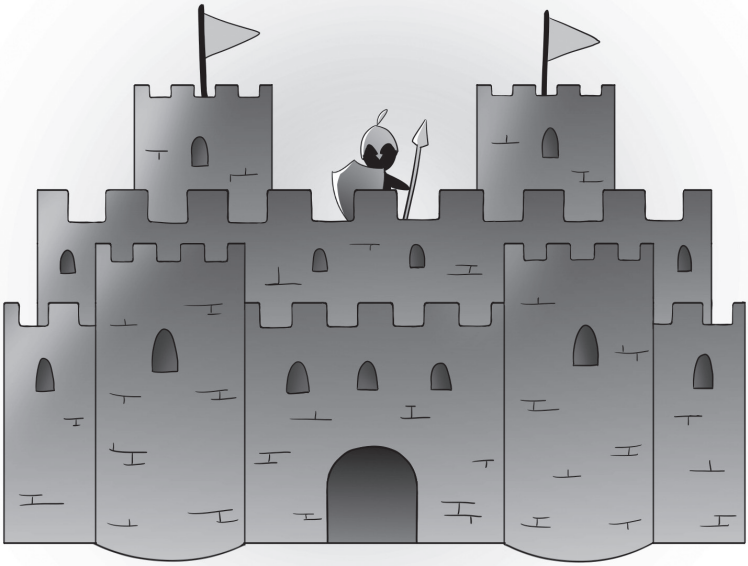
Ciò ha fatto sì, storicamente, che la sua offerta di mercato si mantenesse sempre costante e controllata, consentendogli di conservare, se non addirittura di incrementare, il proprio valore nel tempo, e di guadagnare così lo status di bene rifugio.

Lo stesso non si può dire, ad esempio, delle tradizionali valute fiat, quali l'euro e il dollaro, che per una serie di motivi, tra cui anche il fatto di poter essere create dal nulla in quantità potenzialmente infinite dalle banche centrali, hanno visto il proprio potere d'acquisto ridursi progressivamente nel tempo.

La correlazione tra scarsità e preziosità dell'oro, dunque, spiega perfettamente una delle leggi fondamentali del libero mercato, ovvero quella della domanda e dell'offerta, secondo cui la disponibilità di un prodotto, a parità di domanda e di qualità intrinseche dello stesso, incide notevolmente sul suo valore percepito e, in definitiva, sul suo prezzo.

Se infatti ipotizzassimo, per assurdo, che da un giorno all'altro venissero scoperti migliaia di giacimenti d'oro dislocati geograficamente in tutto il mondo, dai quali il nobile metallo potesse essere facilmente accessibile ed estraibile, allora il suo valore crollerebbe, proprio perché le sue caratteristiche di rarità e inaccessibilità verrebbero meno.

Al contrario, se tutti i giacimenti auriferi attualmente presenti sul nostro pianeta dovessero improvvisamente esaurirsi, bloccando definitivamente l'afflusso di nuovo oro nel mercato, allora il suo prezzo schizzerebbe alle stelle, dal momento che diverrebbe ancor più raro di quanto non lo sia già oggi.



Fonti principali

Capitolo 1

La storia di Kane Gamble: https://www.judiciary.uk/wp-content/uploads/2018/04/r-v-gamble-sentencing.pdf.

Capitolo 2

Libro: *Le armi della persuasione. Come e perché si finisce col dire di sì*, Robert Cialdini, Giunti Psychometrics, Enlarged edizione, 2022

La storia di Debby: cfr. fonti del capitolo 3

Capitolo 3

Libro: *The woman behind the smile. Triumph Over the Ultimate Online Dating Betrayal*, Debby Montgomery Johnson, Parker House Publishing, 2016

Intervista: https://whatismyipaddress.com/surviving-a-romance-scam-with-debby-montgomery-johnson

Dati FBI: https://www.fbi.gov/contact-us/field-offices/houston/news/press-releases/1-billion-in-losses-reported-by-victims-of-romance-scams

Capitolo 4

Storia di Gavin: https://people.com/crime/brandon-guffey-son-sextortion-victim-died-by-suicide/

Storia di Ryan: https://edition.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html

Comunicato polizia postale: https://www.commissariatodips.it/notizie/articolo/sextortion-cresce-il-numero-dei-minori-vittime-di-sextortion/index.html

Capitolo 5

FAAC: Articoli vari da web

Corcoran: Articoli vari da web

Capitolo 6

Bitcoin: Whitepaper Bitcoin: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

Twitter scam: Complaint court form: https://www.justice.gov/d9/press-releases/attachments/2020/07/31/sheppard_complaint_0.pdf

Affidavit Fazeli: https://www.justice.gov/d9/press-releases/attachments/2020/07/31/fazeli_complaint_0.pdf

Capitolo 7

Scam Pandora: Articoli vari da web

Capitolo 8

Articolo «the Guardian»: https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause

Informatica | Psicologia

dello stesso argomento

Flavia Montanile, Massimo Montanile, *Un modello per la sicurezza dei dati personali nell'era digitale*, 978-88-9295-090-0 (ISBN edizione digitale 978-88-9295-100-6)

Pasqualina Florio, *Terrorismo cibernetico e sicurezza nazionale. Potenziale metamorfosi della minaccia eversiva*, 978-88-9295-724-4 (ISBN edizione digitale 978-88-9295-725-1)

Fabio Leuzzi, *Ars intelligendi* (seconda edizione in corso di pubblicazione)

Nella mente dell'hacker. Tecniche di persuasione e manipolazione mentale in rete
di Luigi Gobbi
illustrazioni di Milian Zheng
prefazione di Giovanni Ziccardi

direttore editoriale: Mario Scagnetti
editor: Marcella Manelfi
caporedattore: Giuliano Ferrara
redazione: Sara Ferretti
progetto grafico: Sara Pilloni