Carloalberto Sartor

CONOSCO LA TUA PASSWORD

Manuale di autodifesa informatica

Come difendersi dagli hacker, riconoscere ed evitare le truffe informatiche, proteggere il proprio conto corrente online, evitare di cedere informazioni utili su di noi

EDIZIONI IL PUNTO D'INCONTRO

Carloalberto Sartor

CONOSCO LA TUA PASSWORD

Manuale di autodifesa informatica

Come difendersi dagli hacker,
riconoscere ed evitare le truffe informatiche,
proteggere il proprio conto corrente online,
evitare di cedere informazioni utili su di noi

Virus, trojan, phishing, malware,
spam, miner: gli agguati della Rete.
Dark Web: la nuova frontiera sommersa

EDIZIONI
IL PUNTO
D'INCONTRO

Indice

Premessa

Che razza di libro è questo?

Un libro per tutti coloro che, per un motivo o per l'altro si trovano ad aver a che fare con computer, smartphone o altre diavolerie informatiche. Sono tutti marchingegni che spesso ci troviamo a utilizzare per forza, controvoglia o comunque "*perché non se ne può fare a meno*".

Senza computer o smartphone, ormai, si sarebbe tagliati fuori dal mondo, impossibilitati a fare qualunque cosa, dal prenotare un viaggio al vedere l'estratto conto. Oggi ognuno di noi ha una mail da leggere o deve entrare in qualche sito. La quantità di cose che si fanno usando il computer o un'app dello smartphone è praticamente infinita.

La pandemia ha dato il colpo di grazia a chi preferiva averci il meno possibile a che fare: smart working per gli adulti, didattica a distanza per chi studia, medici o uffici pubblici con cui anche solo per prenotare un appuntamento devi avere dimestichezza con computer, password, app e autorizzazioni...

Viviamo sempre più in un mondo digitale in cui SMS, WhatsApp, siti o social network sono ormai obbligatori e non solo per contattare gli amici o per condividere i selfie di una festa. Siamo diventati esperti (a volte per obbligo più che per diletto o per risparmio) negli acquisti online, seguiamo la consegna dei pacchi nel sito del corriere, prenotiamo online una visita medica o un tampone e ne vediamo online il referto. C'è chi ha sempre avuto dimestichezza e confidenza con l'informatica e chi invece ne farebbe volentieri a meno. Per tutti, comunque, esiste l'incubo della password, del pin, delle credenzia-

li, dello SPID (aaaargh!): tutte cose inventate per impedire che un hacker possa entrare nei computer, rubare qualcosa, danneggiare, infettare, bloccare. Ma ogni tanto ci coglie il dubbio che avvenga il contrario, perché, per colpa della password, spesso noi non riusciamo ad accedere. L'hacker invece ci riesce lo stesso!

E se sulla password ci sono già molte cose da dire, sugli hacker ce ne sono molte di più, visto che se ne sente sempre più parlare. E non bene! Ecco quindi qualcosa da leggere per farsi un'idea di come sopravvivere in questo mondo tecnologico!

Introduzione

Non è semplice sopravvivere digitalmente! Tra posta aziendale e personale, social vari, Facebook, Twitter, Telegram... è tutto un fiorire di password da gestire e da ricordare!

Poi ci sono le password dei computer d'ufficio e di casa, quelle degli smartphone, le password degli accessi per lo smart working, la didattica a distanza... Compri un televisore e anche su quello c'è un codice d'accesso. Poi c'è il Wi-Fi, lo SPID, il bancomat. E ogni due per tre anche lo smartphone ti chiede un codice per questa o quella app. Non manca ogni tanto l'autorizzazione via SMS, anche quella con un codice. E infine l'app della banca, che ti chiede un codice per confermare il pagamento... ma quante password servono per vivere?

E di password, appunto, parla il titolo. Una parola evocativa di tutta una serie di problematiche di sicurezza che in un qualche modo troverete raccontate, spiegate, vissute.

Parleremo qui di tante cose, tra cui, per esempio, virus, intrusioni informatiche, accessi abusivi; troverete furti di dati e reati informatici di vario tipo.

Uno dei temi centrali è sicuramente quello degli hacker, di cui sentiamo spesso parlare sui giornali, alla televisione o da qualcuno che direttamente o indirettamente ci ha avuto a che fare. A parte la percezione che l'hacker combini dei gran disastri, non ci è ben chiaro cosa fare esattamente per evitarli e, soprattutto, come evitare di incapparci direttamente!

L'informatica è vasta e articolata e anche il mondo degli hacker lo è. Anzi, essendo gli hacker sostanzialmente molto più creativi della media

degli esseri umani, il loro contesto è ancora più articolato e complesso di quello che ci immaginiamo e sono sempre pronti a sorprenderci.

Parleremo di attacchi informatici grazie a vari esempi che spero possano dare un'idea del tipo di nemici con cui abbiamo a che fare, con i loro spesso imprevedibili tranelli, fatti anche inviandoci link a siti sconosciuti o facendo circolare fake news (molto usate!). Ma cercheremo anche di far capire la loro mentalità e le loro capacità di prevedere le nostre azioni.

Il primo ingrediente del problema

La mia personale esperienza di informatico mi ha portato col tempo a capire che gli hacker, per compiere le loro malefatte, contano sul fatto che noi utilizzatori non abbiamo la più pallida idea delle loro strategie, delle loro tecniche e tantomeno abbiamo un'idea dei loro obiettivi. Ogni volta che gli hacker fanno scattare la loro trappola, noi ci caschiamo facilmente. La nostra inconsapevolezza su cosa fanno gli hacker è quindi il primo ingrediente del problema.

Il secondo ingrediente del problema

Gli hacker, per evitare di essere scoperti, entrano nei computer delle vittime passando attraverso i nostri computer, grazie a qualche debolezza nella loro sicurezza o usando qualche trucco per renderli deboli. Noi non ce ne accorgiamo, anche perché l'hacker, da buon parassita, cercherà di non crearci problemi, in modo da poter "viaggiare a sbafo" verso i computer delle vittime.

Questa nostra *inconsapevole collaborazione* permette all'hacker di attaccare altri computer e di combinare i disastri di cui sentiamo parlare ormai ogni giorno nelle cronache.

Ecco qual è il secondo ingrediente del problema. Senza saperlo gli diamo una mano! Cosa possiamo fare per migliorare la situazione?

Io, nel mio piccolo, ho pensato tante volte che, da informatico, potrei provare a raccontare alcune cose su questo strano mondo, sulle tecnologie, sugli hacker. Spiegare cosa succede, dare delle indicazioni. Sferrare un pugno ai due ingredienti del problema che abbiamo visto sopra.

Non tutti possono fare un corso specialistico su questi argomenti, quindi queste pagine potrebbero essere un punto di partenza, in cui magari trovare qualcosa di utile.

Non è che degli hacker e delle loro malefatte non se ne parli mai, anzi. Sempre più spesso le cronache ci parlano di attacchi, aziende bloccate, truffe informatiche e conti correnti svuotati. Non sono nemmeno pochi i thriller polizieschi o tecnologici che ne parlano, solo che ne tratteggiano le "imprese" in un modo che non ha molto a che fare con la nostra vita di tutti i giorni e che non ci fornisce alcun trucco per sopravvivere alle loro malefatte.

Non ci mettono veramente in grado di cogliere il modus operandi degli hacker.

Apprendere che se stai più di trenta secondi al telefono la CIA riesce a scoprire dove ti trovi (e che la stessa cosa può fare anche l'hacker che appartiene a una banda criminale) non è poi molto utile all'uomo della strada per evitare una truffa o all'azienda per evitare che un hacker cancelli tutti i dati aziendali e poi chieda il riscatto. Non ci evita di trovarci i conti correnti alleggeriti dal furbone di turno.

Ecco perché ho deciso di parlarne in tutt'altro modo e di cercare di spiegare il contesto in cui lavorano e i trucchi che mettono in atto.

Siamo tutti vittime

Chiunque può essere vittima di un hacker. Abbiamo anche capito che possiamo essere vittima e contemporaneamente inconsapevoli collaboratori. Possiamo esserlo mentre lavoriamo, mentre siamo a casa, quando siamo in ferie, la sera mentre guardiamo un film al computer e in qualunque momento della giornata.

Anche noi addetti ai lavori siamo a rischio. Con le stesse debolezze, ma, attenzione, non con gli stessi rischi, in quanto, siamo molto più bersagliati dagli hacker rispetto agli altri. Un hacker che riuscisse a conquistare il computer di un informatico che lavora per un'azienda, potrebbe accedere ai vari sistemi dei clienti di quell'azienda. Potrebbe attaccare infrastrutture importanti, acquisire dati riservati, effettuare attività cui i normali utenti non sono abilitati. Gli episodi di cronaca (oltre alle statistiche!) sono lì a mostrarcelo.[1]

Lo dico "esperienze personali alla mano", ma anche sulla base dell'esperienza di tanti colleghi: noi addetti ai lavori siamo ugualmente poco consapevoli di come gli hacker operano e possiamo quindi essere vittime di un hacker senza rendercene conto, esattamente come il cosiddetto "uomo della strada".

Chissà che queste pagine possano essere utili anche a qualche mio collega informatico, sicuramente competente ed esperto in vari campi ma, magari, non troppo preparato su questo specifico argomento.

Ecco perché, senza perdermi troppo nei tecnicismi, vorrei rendervi meno oscuro il modo con cui l'hacker perpetra i suoi attacchi e cercare di agevolarvi nel riconoscere (o almeno evitare) le più comuni situazioni a rischio. Cercare di aumentare la consapevolezza su questi fenomeni semplicemente raccontando come avvengono determinate azioni degli hacker può servire ad aumentare l'attenzione su questi fenomeni e dare un contributo? Me lo auguro!

In questo libro troverete tra le tante cose anche la descrizione di incursioni tecnologiche di tipo meno noto, delle quali magari non avete mai sentito parlare e che mai avreste immaginato potessero esistere.

La realtà, infatti, supera ampiamente la fantasia, lo sapete. Quindi troverete anche qualche dettaglio che vi sembrerà decisamente incredibile: dalle gare tra hacker che si svolgono sui computer di tante persone come noi ad altri hacker, decisamente più altruisti, che entrano

---

1 Gli attacchi provenienti da computer di dipendenti: https://www.corrierecomunicazioni.it/cyber-security/attacco-hacker-lazio-damato-e-partito-dallutenza-di-un-dipendente-in-smart-working/

nel vostro computer per eliminare un pericoloso virus che potrebbe abbattere il vostro computer o quello di qualcun altro.

Non mancheranno i banali (ma sempre attuali) casi di dipendenti infedeli che rivendono ai concorrenti i segreti industriali della loro non più amata azienda e, allo stesso modo, troverete anche traccia di incidenti tecnici assurdi che permettono agli hacker di "arraffare tutto".

Conoscerete inoltre altre ulteriori stranezze, molto appetibili per i più accaniti complottisti: enti di sicurezza che progettano visite nel vostro computer alla ricerca di terroristi a cui gli hacker rubano progetti e strumenti di attacco e hacker che cercano di avvelenare migliaia di persone.

Avremo anche modo di ricordare alcuni scienziati sconosciuti, grazie ai quali l'informatica ha potuto nascere e svilupparsi. Troverete infine qualche descrizione di tempi antichi, nei quali, pur non essendoci internet, le interazioni erano molto "social".

Molti fatti sono qui descritti con nomi di fantasia, ma anche ricorrendo a ricostruzioni romanzate, per evitare di rendere troppo pesante la lettura, oltre che per evitare che le vittime possano essere riconoscibili.

Questo libro non è una bibbia!

Questo libro non è (e non può essere) una specie di "bibbia" o un manuale di cybersecurity per addetti ai lavori. Si tratta di uno strumento concepito per aiutare le persone a capire come utilizzare in sicurezza i diversi sistemi informatici che, per lavoro, per svago o per varie necessità ci si trova a utilizzare.

L'ho scritto nella convinzione di poter dare suggerimenti, consigli e soprattutto stimoli che permettano di maneggiare con maggiore sicurezza (e minori patemi!) i vari tipi di sistemi informatici con cui abbiamo a che fare tutti i giorni, spesso per parecchie ore al giorno.

Tra l'altro i sistemi informatici ormai circondano letteralmente la nostra esistenza, quindi che sia per lavoro, per svago ma anche per

comunicare con amici e parenti, per prenotare una vacanza o per usare l'automobile, ci troviamo sempre tra i piedi un qualche tipo di computer.

E dove c'è un computer, un sito o un qualche tipo di programma, ecco che ci vuole una password o un codice per farsi identificare dal sistema. Un ostacolo odioso che però non nasce a caso: serve per evitare che qualcun altro, al nostro posto, utilizzi qualcosa che è meglio resti di nostro possesso e uso esclusivo, come le chiavi di casa, i documenti di identità, la password, il PIN o le credenziali. Utili strumenti che impediscono (o rendono abbastanza complicato) a degli sconosciuti di entrare a casa nostra o nelle "nostre cose".

Nella mia quotidiana esperienza incappo spesso in incidenti di sicurezza che sono causati da errori compiuti dagli utenti nel definire o utilizzare le credenziali. Ecco quindi la necessità di sensibilizzare chi non è un addetto ai lavori su questi argomenti, aiutandolo a prendere coscienza dei pericoli rappresentati dagli hacker, di cui cercherò di raccontare in modo comprensibile tecniche e modus operandi.

> *Non si tratta (magari bastasse) di imparare a memoria una serie di regole, perché l'estrema varietà e articolazione del problema degli hacker richiederebbe un elenco di regole decisamente complesso, lungo e irto di sottoregole legate a mille condizioni diverse. Molto meglio ricevere una adeguata serie di stimoli, riuscire a entrare nella logica di questi problemi, avere un minimo di conoscenze di contorno, avere presenti alcuni esempi, essere in grado di diventare il più possibile autonomi.*

Notevoli le semplificazioni che troverete in questo libro. Indispensabili per non rendere troppo complesso leggerlo. Userò esempi che magari faranno sorridere per la loro banalità. Meglio così, resteranno impressi. Userò il meno possibile sigle e informatichese. Non è semplice farlo ma ci provo.

Sarebbe bello poter scrivere un libro con tanto rigore accademico. Ma a parte il riuscire a farlo (che non è semplice), risulterebbe illeggi-

bile per la maggior parte delle persone a cui questo libro è dedicato o, alla terza pagina, verrebbe immediatamente promosso al ruolo di soprammobile.

Occuparsi anche del fattore umano

Sono un addetto ai lavori, pieno di passione per le tecnologie informatiche e per la cybersecurity. Il mio lavoro principale è oggi quello di identificare hacker, virus e altre stranezze nei computer delle aziende che mi chiamano per sapere se hanno delle "sorprese" al loro interno.

Per farlo uso vari strumenti, tra cui uno particolare che ho scritto appositamente, concentrando al suo interno tutto ciò che l'esperienza professionale mi ha suggerito nell'arco di alcuni decenni di attività. Si tratta di uno strumento che reputo molto efficace e che, sul campo, mi ha permesso di scoprire e neutralizzare vari hacker, identificare i loro virus, scoprire le debolezze delle reti e dei computer, perché nonostante il grande spiegamento di mezzi, le tecnologie eccelse, la carta patinata per pubblicizzare futuristici servizi di sicurezza, la realtà ci dice a chiare lettere che i sistemi di sicurezza messi in campo dalle aziende non riescono ancora a dar loro sufficiente sicurezza e tranquillità a chi usa i sistemi.

Se da una parte è sicuramente difficile progettare le opportune difese informatiche per un'azienda, dall'altra è pure facile compiere banali (= umani) errori nel metterle in opera, per cui un "check-up" per capire in che stato si trova è sempre cosa utile. Ed è una operazione che raccomando di fare con una certa frequenza.

Professionalmente ho seguito vari casi particolari e importanti, studiando il contesto, le intrusioni e le metodologie di lavoro degli hacker, ma ogni giorno che passa mi rendo conto che per affrontare gli hacker i tecnicismi non sono tutto, visto che basta a volte un banale errore di un utente qualunque per vanificare le difese aziendali e aprire la porta all'hacker. Altrettanti rischi sono generati da chi amministra i sistemi, i

servizi, le credenziali e le reti. Basta una svista: la porta blindata si apre e può entrare qualcuno.

Il fattore umano gioca quindi un ruolo fondamentale. Sia per gli addetti ai lavori, sia per coloro che sono semplici utilizzatori del computer e dei servizi informatici, per lavoro o per diletto.

Corsi, formazione, aggiornamenti continui sul tema sono indispensabili. Gli attuali attacchi degli hacker non sono quelli di un anno fa. Se ne sono aggiunti di nuovi, se ne sono modificati altri. Basta digitare le credenziali nel posto sbagliato (una pagina di un sito che ci sembra il solito ma non lo è) ed ecco che la sicurezza dell'intera azienda può essere compromessa. Ma questo vale anche per l'home banking familiare, per la nostra casella di posta personale, per l'account sui social (Facebook, Instagram eccetera) o qualunque altro "luogo digitale" di uso personale.

Basta anche installare un programma, magari su suggerimento di uno sconosciuto. Qualcosa di cui ci viene decantata l'utilità. Bello, utile e perfino gratuito, ma potrebbe essere un programma che comunque "fa anche altro" o è infetto. A volte il programma, incensato come "il migliore per difendersi dagli hacker", ci appare su un social o leggendo un sito e ciò abbatte la nostra diffidenza.

Infine, da quando lo smart working ha preso piede (la pandemia, sigh), il molto insicuro territorio informatico domestico è diventato anche territorio lavorativo e l'insicurezza aziendale è aumentata invece di diminuire.

Il ricorso emergenziale al "lavoro agile", senza dare il tempo di organizzarlo per bene, ha ulteriormente peggiorato la situazione. Di giorno, il dipendente lavora in smart working col suo pc domestico (chissà come era messo, in termini di sicurezza) e magari di sera i figli caricano il gioco "taroccato" sullo stesso computer, introducendo chissà quali rischi al computer domestico. Il mattino successivo il dipendente si connetterà alla rete aziendale e magari ci trasferirà l'infezione di turno.

Ecco quindi che l'esperienza suggerisce di prendersi altrettanta cura degli aspetti umani. Fondamentale che anche i non addetti ai lavori

possano avere un'idea meno oscura dei meccanismi e delle tecnologie. Una comprensione delle tecniche usate dagli hacker, seppure senza entrare nei dettagli tecnici, può essere molto utile per evitare agli utenti di cascare nelle loro trappole.

Un hacker che riesca a far compiere a un utente una attività specifica, per quanto semplice e apparentemente innocua, può riuscire ad azzerare le difese tecnologiche di sicurezza dell'intera azienda.

Ecco perché trovo naturale affiancare alla mia "lotta contro gli hacker" una parallela consistente attività di divulgazione "per l'uomo della strada". Un po' come farebbe un buon medico che sa usare le medicine per curare il paziente, ma sa anche che con qualche saggio consiglio potrebbe evitargli tante future malattie. E magari fare in modo che capisca quando è il caso di rivolgersi a lui, prima che i guai diventino più grandi e più difficili da curare.

Spero quindi che possiate leggere questo libro anche con leggerezza, nel tempo libero, trovandoci una chiave di lettura di un mondo decisamente strano in cui ci troviamo a vivere grazie alle nuove tecnologie. In cui siamo immersi ormai ventiquattr'ore su ventiquattro!

Non resta che allacciare le cinture di sicurezza (informatica) e iniziare il viaggio!

Che strano titolo

A molti è capitato di ricevere una mail in cui un tizio (a volte addirittura spacciandosi per la polizia) dice che vi ha osservato per un bel po', che vi ha visto scorrazzare su siti porno "vietati", che ha letto i vostri documenti, che sa chi siete e che potrebbe raccontare ai vostri contatti che cosa fate nella vostra vita privata e quali turpi siti frequentate. Aggiunge sempre "*Conosco la tua password*". Vi ricatta, in soldoni, chiedendovi di pagare una multa per evitare scioccanti indagini giudiziarie a vostro carico o figuracce mortali con parenti e amici o divorzi dolorosissimi... o magari vi chiede di installare un programma che cancelli i dati peccaminosi che si trovano sul vostro computer. Sta millantando,

ovviamente. Non fate nulla di quello che dice. Non entrate nel panico e non fate mosse azzardate.

Ha scritto a voi semplicemente perché in Rete ha trovato in un qualche modo il vostro indirizzo di posta. Ha scritto a voi, ma ha scritto la stessa cosa anche a tutti gli altri indirizzi di posta che ha trovato. Di voi non sa nulla. Ci prova, attribuendovi qualcosa che un tot di persone effettivamente fa, dando quindi a molti destinatari di questa mail la sensazione che ciò che scrive è vero e che effettivamente ha accesso al loro computer. Del resto, se inviate una mail a cento sconosciuti con scritto dentro "So che sei tifoso della Juventus" (o del Milan o di una qualche squadra nota), magari una decina o ventina di persone si chiederanno effettivamente come fate a saperlo.

Beh, ecco spiegato perché il libro ha questo titolo!

Capitolo 1

L'influenza degli hacker nella nostra vita

Ce ne rendiamo vagamente conto solo quando balza agli onori delle cronache per qualche episodio eclatante, di fatto lontano dalla nostra vita quotidiana. "*Accade altrove e a qualcun altro*". Non ne sentiamo il fiato sul collo e, per questo motivo, non mettiamo in atto idonee contromisure per non esserne vittime.

Questa distorta percezione non appartiene a una qualche nostra inconsapevolezza generale o fiducia estrema nel genere umano. Non siamo imprudenti in assoluto. Infatti quando usciamo di casa chiudiamo la porta a chiave. La nostra bici ha il lucchetto. Quando usciamo dall'auto la chiudiamo in modo che non ce la rubino. Stiamo normalmente attenti a non farci derubare per strada e, se vediamo una persona il cui atteggiamento ci appare minaccioso o comunque pericoloso, ci comportiamo in modo adeguato.

Se incontriamo qualcuno che ci porge una banconota da 100 euro dicendo: "*Tieni, te la regalo!*", arretriamo insospettiti, senza toccare i soldi. "*Sarà sicuramente una truffa!*", pensiamo, perché nessuno ti regala dei soldi.

Sono le normali attenzioni dettate dalla nostra personale esperienza; derivano dalle raccomandazioni fatteci dai nostri genitori, emergono dalle indicazioni, dai consigli e dalle esperienze di persone che fanno parte della nostra cerchia, dalle quali "abbiamo appreso" che ci sono dei pericoli da evitare, da prevenire.

Quando siamo al computer, chissà per quale motivo, tante delle nostre prudenze e attenzioni sembrano cadere del tutto o almeno sono

molto mitigate. Sarà forse perché al computer tutto è virtuale: siamo a casa nostra, tranquillamente seduti davanti al computer e non può accaderci nulla di grave! Anche con lo smartphone, magari sul divano di casa o in giardino... pensiamo di essere comunque al sicuro?

Sarà magari che in questa situazione nessuno ci può puntare la pistola alla tempia, minacciarci o rapinarci, cosa che invece per strada (un luogo notoriamente non troppo sicuro) potrebbe succedere. Oppure, pur coscienti di molti dei rischi che possiamo correre mentre viviamo dentro i social, riteniamo di essere "*troppo poco interessanti*" per un hacker e non ci preoccupiamo di finire nel loro mirino?

Difficile trovare una spiegazione esatta e convincente. Sta di fatto che le nostre imprudenze digitali sono ampie e gli hacker le sfruttano. Il nostro computer (con cui interagiamo allegramente e imprudentemente) diventa lo strumento con cui gli hacker entrano a casa nostra, spesso senza nemmeno cercare di sfondarla, perché siamo noi ad aprirgliela!

Addirittura, tornando all'esempio dello sconosciuto che ci porge la famosa banconota, ci appropriamo di tante cose in Rete (programmi, giochi, musica, filmati e altri beni che sicuramente hanno un costo non indifferente) attratti dalla scritta *gratis*, senza alcun sospetto su questa "banconota" che comunque ci viene offerta in continuazione, apparentemente senza alcun tornaconto.

Così un gioco gratuito (che è costato centinaia o migliaia di ore di lavoro a qualcuno) noi non ci facciamo scrupoli a usarlo e nulla ci domandiamo, appunto per il fatto che è gratis. Ma perché è stato realizzato? Con quali obiettivi? Dov'è la convenienza per chi l'ha fatto, visto che non tiriamo fuori un centesimo? Eppure quel gioco gratuito è esattamente come quella banconota che, offertaci di persona, ci farebbe allontanare subito la mano!

Un atteggiamento meno imprudente, con qualche riflessione attenta, ci potrebbe fornire una chiave di lettura (e di comportamento) sia per quanto riguarda i social, sia per quel che riguarda le persone che lo popolano e che non sempre interagiscono con noi per amicizia, conoscenza o interessi comuni.

Altrettanta prudenza, sui social, dobbiamo metterla sulle notizie che ci capita di leggere. Emesse da chi? Con quale attendibilità? Con quali obiettivi?

Nella nostra imprudenza e innocenza, non facciamo caso al fatto (a noi ben noto) che i social spendono centinaia di milioni di euro all'anno per permetterci di salutare gli amici, scambiarci ricette, immortalare in un selfie il gruppetto di amici con le birre in mano, dire la nostra sui più svariati temi, far conoscere ai propri contatti i luoghi in cui si va in ferie eccetera.

Non possiamo credere alla favoletta dell'ente di beneficenza che ci permette di comunicare senza che vi sia un qualche interesse. Il social non sarebbe quotato in Borsa, non avrebbe degli investitori che ci mettono dei soldi per raccoglierne ancora di più alla fine dell'anno.

Come mai il social ci mette a disposizione tutte queste costosissime tecnologie? Evidentemente perché ci guadagna! Altrimenti gli investitori sarebbero fuggiti a gambe levate. Quindi le nostre gite, i nostri pensieri, le birre e le spiagge che frequentiamo, i nostri selfie e la foto del cane o della motocicletta nuova che abbiamo orgogliosamente pubblicato per condividere la nostra vita con i nostri contatti, hanno un valore? Certo! Qualcuno le vende a qualcun altro.

C'è anche la pubblicità che sotto traccia scorre tra le pagine che guardiamo. Pubblicità che è molto intelligente, visto che se parliamo spesso di barche ci arriverà pubblicità di quel tipo. E i siti di fake news, con titoli catastrofici o complottisti, attirando sapientemente il nostro "click", hanno veramente l'obiettivo di farci sapere questa o quella notizia o a loro interessa il nostro click e basta? E più diventiamo incapaci di discernere il vero dal falso, più saremo portati a cliccare sulle fake news, assetati di novità? Quante volte i siti di fake news sono stati usati non solo per "manipolare le masse", ma anche per veicolare infezioni informatiche?

Sono molte le domande che dovremmo farci mentre viviamo in questo strano mondo virtuale dove molte cose non sono come sembrano.

Quindi i social ci hanno "disorientato" e a loro noi cediamo gratis tutto ciò che siamo, che pensiamo, che facciamo. Usiamo dei server che hanno costi pazzeschi e non spendiamo una lira? Ohibò! L'informa-

tica ha questi e altri effetti. Le tecnologie modificano le nostre reazioni e sensazioni in modo spaventosamente silenzioso, abbassando drasticamente la soglia dei nostri meccanismi di controllo.

Fake news

Leggiamo una notizia strana? Beh, se l'hanno scritta, sarà vera! Così quel documentario molto interessante e ben confezionato in cui ci raccontano che una certa cosa, una certa tendenza, un credo politico, una specifica critica "al sistema" o alla politica, una notizia che mette in cattiva luce una persona, un'azienda, uno stato, un comportamento ecc. sarà costato del lavoro, del tempo, attori, comparse, il tempo non banale per confezionarlo. Siamo sicuri che non ci sia qualcosa dietro? Quante volte una notizia che svela un oscuro complotto potrebbe essere parte a sua volta di un complotto (questa volta vero!)?

Siamo altamente sensibili ai complotti, ai segreti, alle verità nascoste. Al punto che quando leggiamo da Stellina84 quali sono le segretissime ma reali intenzioni di questo o quel politico siamo convinti che Stellina84 sia depositaria della verità e sappia tutto quello che ci viene nascosto dal sistema. Ma è possibile che Stellina84 abbia accesso ai segreti più inconfessabili e meglio celati al mondo e li possa tranquillamente apprendere e pubblicare sul suo account?

Forse dovremmo andare a leggere i bilanci di tante aziende, di tanti partiti o di qualche "centro di potere". Ci troveremmo grosse spese investite nei social e non sapremo mai bene a cosa servono quelle spese. Forse a manipolarci?

Lecito e illecito: concetti che sbiadiscono

Non solo perdiamo il senso critico sulle notizie che leggiamo. Perfino il nostro rapporto con il lecito e l'illecito viene stravolto dalle tecnologie, con un impatto culturale trasversale molto pericoloso. Il concetto di

proprietà (e tutti gli aspetti legali relativi), per esempio, si trasforma in modo notevole, per motivi legati alla virtualità delle tecnologie. Siamo abituati a fare una "copia" delle cose senza mai fare un parallelo con i pensieri che avremmo fatto in passato, prima dell'avvento del computer.

Domande come "*Mi appartiene?*" non ce le facciamo spesso. "*Tizio ha lavorato per farlo, se me lo prendo devo pagarlo!*" non è un pensiero che ci governa, eppure nel mondo fisico questo tipo di domande scatta immediatamente ma, chissà perché, nel mondo virtuale le domande più ovvie non ce le facciamo.

Un genitore che vede un figlio che ruba qualcosa a qualcuno, anche se fosse un furto insignificante in termini di valore economico, gli farà sicuramente una bella lavata di capo, per fargli comprendere che si tratta di qualcosa che non va assolutamente fatto, che è un illecito, un torto verso un'altra persona. Condirà la cosa con molti concetti, tra cui quello del "non fare agli altri quello che non vorresti fosse fatto a te", della necessità di rispettare il lavoro altrui e di riconoscergli un valore... e altri mille concetti etici che stanno alla base della nostra vita di relazioni, fondata tra le altre cose sul rispetto assoluto della proprietà altrui.

Lo stesso genitore, oggi, quando suo figlio quattordicenne scarica da internet giochi piratati o riesce a vedere gratis la partita di calcio che sarebbe fruibile solo agli abbonati di questo o quel servizio, non è detto che abbia la stessa reazione, sempre se si rende conto di ciò che combina suo figlio.

Paradossalmente potrebbe essere molto contento per le prodezze tecnologiche del figlio, che permettono alla famiglia di risparmiare... sarà perfino contento che il figlio possieda queste abilità ("potrebbe diventare un lavoro") e si siederà soddisfatto a guardare la partita rubata da un qualche pirata informatico e messa a disposizione degli altri, magari a piccole cifre.

Il seguito di questa storia forse non ha le ricadute attese e il figlio, dopo qualche anno, potrebbe diventare un pirata informatico di professione, magari guadagnando molto più del compagno di scuola che lavora in un call center per pochi euro all'ora. Oppure a un certo punto

suonano alla porta ed è la Guardia di Finanza che ti notifica un atto decisamente sgradevole che riguarda le abilità e furbizie di tuo figlio[2] e le partite che hai visto gratis o a pochi spiccioli adesso te le faranno pagare molto salate.[3] Se tuo figlio avesse prelevato materialmente a casa di qualche sconosciuto dischi, film o giochi e avesse allestito un mercatino davanti a casa, sicuramente lo avresti preso per l'orecchio obbligandolo a restituire tutta la refurtiva. Le tecnologie ottenebrano le nostre menti e il nostro raziocinio!

Chi come l'hacker ha capacità di maneggiare tecnologie e persone per perseguire i propri obiettivi ha un enorme spazio di azione che in parte è costituito dalla nostra ignoranza, oltre che dalla nostra leggerezza. Gli altri ingredienti che gli hacker hanno in mano li vedremo più avanti.

L'intrusione

Una delle cose più importanti che l'hacker cerca di fare è quella di "entrare" nel nostro computer, dove potrà trovare tante cose utili per le sue malefatte. Questo accesso, chiamato *intrusione*, può avvenire in molti modi diversi.

Un'altra cosa cui l'hacker aspira è costituito dal poter entrare nei servizi digitali ai quali noi siamo iscritti e per i quali abbiamo un accesso specifico a noi riservato. Servizi che utilizziamo inserendo una password, un pin, delle credenziali (nome utente e password) o usando un qualche altro meccanismo di identificazione.

Tutti noi usiamo posta elettronica, home banking, acquistiamo online, spediamo e riceviamo documenti (sono solo alcuni banali esempi, i più comuni per il cittadino qualunque). Dove potrebbe esserci un fattore di rischio nel caso uno di questi servizi venisse intruso da un hacker? Facciamo qualche esempio. Entriamo nell'home banking per emettere bonifici: attività che ci sembra inoffensiva. Peccato che se un hacker

2 https://www.punto-informatico.it/italiazip-partite-denunce-per-il-p2p/

3 https://www.hdblog.it/mobile/articoli/n538460/iptv-illegali-italia-sanzioni-utenti-abbonati/

riuscisse a entrare nel nostro home banking potrebbe inviare a un suo conto corrente tutti i soldi che sono nella nostra disponibilità (compresi quelli che non ci sono veramente, ma che la banca ci concede per "sconfinare" in caso di necessità). Danni prodotti dall'hacker? Conto svuotato, anzi, con lo sconfino da pagare! Accade spesso, questo tipo di attacco. Si definisce *attacco diretto*, perché l'hacker attacca direttamente il punto critico, quello dove ci sono i soldi.

Qualcuno potrebbe replicare che il caso dell'home banking è un caso particolare; che altri servizi non hanno questa criticità. "*Cosa vuoi che possa fare un hacker entrando nella posta elettronica di Tizio o Caio?*". Semplice: supponiamo che tu viva in un appartamento in affitto. L'hacker intrude la casella di posta del tuo padrone di casa e ti scrive un messaggio di questo tipo:

```
"Buongiorno!
Segnalo ai condomini che dal mese prossimo le
coordinate bancarie su cui versare l'affitto sono
cambiate. Le nuove coordinate sono le seguenti: xyzkw
Cordiali saluti".
```

Ricevendo questo messaggio, noi faremo un bonifico alle nuove coordinate bancarie, per cui il nostro bonifico verrà inviato al conto che è nelle disponibilità dell'hacker. Una bella truffa!

Si tratta quindi di un attacco di tipo *indiretto*, perché ha intruso informaticamente una persona diversa dalla vittima finale (la casella di posta del proprietario) ottenendo però un risultato "di sponda" (sono sempre io la vittima, quello che perderà i soldi e sarà sempre l'hacker a ricevere i miei soldi, a sbafo!).

Con un'unica intrusione l'hacker ha tra l'altro la possibilità di raccogliere l'elenco di inquilini (del tuo condominio ma anche di altri!) e, cosa molto conveniente, può inviare la stessa mail a tutti gli inquilini, con un ben maggiore risultato economico.

Il furto d'identità

L'unico ingrediente necessario all'hacker è avere accesso alla casella di posta di un soggetto in grado di contattarne altri. Essenziale è che chi riceve le comunicazioni di questo soggetto non dubiti mai del fatto che la casella di posta sia in realtà controllata da un'altra persona. Si chiama *furto d'identità* ed è una cosa che può avere gravissime conseguenze.

Il proprietario di casa non si accorgerà di nulla, anche perché l'hacker avrà cura di cancellare la mail incriminata dalla cartella "Posta inviata", rendendo impossibile al proprietario capire cosa è successo. L'affittuario, non avendo motivi per sospettare, verserà i soldi sul conto indicato e solo quando il proprietario gli chiederà ragione dell'affitto non versato l'incidente sarà recepito. Troppo tardi, sicuramente.

Non percepiamo mai abbastanza chiaramente quale tipo di potere "truffante" un hacker acquisisce accedendo a strumenti informatici in cui circolano fatture, grazie al fatto di poterne dirottare il pagamento. Il caso delle truffe sui condomini non è poi così raro.[4]

Non sempre siamo consapevoli del fatto che possiamo essere vittime o fiancheggiatori di un hacker tramite uno dei vari servizi informatici che utilizziamo. Facciamo infatti molta fatica a comprendere come un semplice account di posta possa permettere azioni così disastrose per noi o per altre persone. E quindi non facciamo nulla per proteggerlo adeguatamente. Quante caselle di posta hanno credenziali stupidissime e, quando sottolineiamo la cosa al suo proprietario, ci sentiamo dire che "*non c'era nulla di importante*"?

L'utilizzo massivo delle tecnologie comporta il fatto che di computer e software siamo ormai letteralmente imbottiti: smartphone, computer, router, tablet, televisori, lettori DVD ma anche decoder per il digitale terrestre, orologi da polso, videogiochi. Per non parlare di altro (pacemaker, dispositivi medicali di vario tipo) che magari abbiamo

4 La truffa a un amministratore di condominio in uno dei tanti casi di cronaca: https://www.ilpiccolo.net/home/2018/11/02/news/nuova-truffa-degli-hacker-con-le-aziende-nel-mirino-7358/

dentro di noi. Ma se saliamo in auto, in moto o su una bici elettrica, siamo sempre alla mercé di uno o più computer, con i loro programmi, le loro debolezze, il loro contenuto informativo spesso molto più importante di ciò che pensiamo.

Tutti questi dispositivi, anche quelli con cui noi utilizzatori non interagiamo direttamente, per motivi tecnici hanno al loro interno un computer che in fabbrica viene configurato e attivato e che, in seguito, potrebbe essere utile/necessario controllare, correggere, riprogrammare o riconfigurare.

Se siamo fortunati, al dispositivo avrà accesso solo chi è autorizzato, grazie a un codice o delle credenziali (nome utente e password). Dovrebbe essere unico e segreto o almeno "riservato" e non indovinabile facilmente, per evitare che ci possa mettere le mani chiunque.

Purtroppo non sempre è così e l'hacker ne approfitta alla grande.

"*Conosco la tua password*": un mantra che l'hacker sembra ripetere in tono minaccioso!

Altri problemi all'orizzonte

Sono molti i punti deboli delle moderne tecnologie che gli hacker assaltano. Tra i tanti, ci sono i futuri (per modo di dire) *robot umanoidi*. Molti di essi verranno progettati e prodotti senza poter prevedere alcune tipologie di problemi legati agli hacker, problemi che oggi facciamo perfino fatica a immaginare, figuriamoci se possiamo implementare dei sistemi per prevederli o evitarli.

Un robot, tanto più se uno di quei modelli sofisticati e attrezzati con logiche di intelligenza artificiale, potrebbe essere intruso da un hacker e manipolato per compiere azioni particolarmente gravi. Per esempio potrebbe impossessarsi di un'arma o compiere gesti pericolosi o fatali per le persone (come strangolare una persona o colpirla con un oggetto contundente).

Situazioni che oggi molti consideriamo eventi da film di fantascienza ma che in realtà costituiscono seri rischi concreti. Come possiamo

arginare un'intrusione su dispositivi di questo tipo? E soprattutto come evitare che, direttamente con una intrusione o indirettamente con dei condizionamenti studiati appositamente, si arrivi al punto in cui il robot compie un gesto "logico" ma con effetti disastrosi?

Sono domande piuttosto pressanti, vista la rapidissima evoluzione nel settore.

Uno dei settori in cui maggiormente ci si preoccupa di questi argomenti è il mercato dei sex-robot,[5] androidi specializzati che, per il tipo particolare di interazione con l'uomo, maggiormente attirano interessi di hacker, vista anche la delicata tipologia di privacy che li riguarda.

Un altro settore tecnologico molto interessato ai rischi indotti dagli hacker è quello della mobilità a guida automatica. Un hacker potrebbe dirottare un mezzo a guida automatica? Con quali conseguenze? Anche il settore aerospaziale sente il fiato sul collo dell'hacking. Dal dirottamento (o peggio, pensiamo allo spegnimento dei motori!) effettuato da un hacker alla possibilità che mandi "fuori orbita" uno delle migliaia di satelliti che ruotano attorno alla terra, facendolo precipitare o collidere con un altro velivolo spaziale.

Le interazioni tra hacker e software di intelligenza artificiale (AI)

Un ultimo argomento di riflessione è quello dell'intelligenza artificiale, ormai ampiamente distribuita in dispositivi, veicoli, robot, dispositivi di controllo, software antivirus, software medico, IoT eccetera. Gli hacker stanno da tempo studiando le possibili "interazioni tossiche" con questo tipo di software. Interazioni che tendono a "condizionare" modelli comportamentali e interpretativi. Il timore è che il passaggio successivo possa essere quello di una vera e propria "manipolazione" degli schemi di apprendimento, di relazione, di azione, con esiti difficilmente prevedibili.

5 I sex robot sono una realtà già oggi! https://www.youtube.com/watch?v=-cN8sJz50Ng

Capitolo 2

Cos'è l'informatica (grazie, Ada!)

L'informatica è una scienza recentissima, con pochi decenni di vita reale rispetto ai millenni di età dell'uomo. La parte per noi più visibile dell'informatica si è sviluppata consistentemente a partire dalla seconda metà del Novecento.

Negli anni '70-'80 l'informatica ha iniziato a diffondersi anche tra i non addetti ai lavori, materializzandosi sempre più sotto forma di "computer" negli ambienti di lavoro, comparendo gradualmente sempre più spesso anche in ambito domestico, come strumento di svago (videogames) oltre che come strumento di elaborazione personale per professionisti ma anche come accessorio per vari e diversificati hobby. Molte persone si sono appassionate alla programmazione e da hobby si sono ritrovati in mano un lavoro!

Alcuni aspetti teorici che governano l'informatica sono nati molti decenni prima dell'invenzione del computer, all'interno di quelle aziende che supportavano il lavoro d'ufficio. Utile ricordare le esigenze di calcolo negli uffici, fino a una certa data coperte tramite calcolatrici meccaniche. Altrettanto utile ricordare le esigenze di redazione testi, inizialmente soddisfatte sempre meccanicamente (macchine da scrivere).

Attorno alla metà del ventesimo secolo presero sempre più piede modelli di computer abbastanza ingombranti, costosi e delicati e contemporaneamente iniziarono a svilupparsi rudimentali tecnologie di trasferimento di testi e immagini (telescrivente, facsimile) che gettarono però le basi per l'invio di questo tipo di dati via radio, a grandi

distanze e anche tramite linee telefoniche. Tecnologie che poi, accluse ai primi computer, permisero un enorme balzo in avanti di tutto il settore informatico, data la grande potenzialità comunicativa che veniva associata alle capacità di calcolo.

Anche se la storia dell'informatica, nel nostro immaginario, è stata scritta da personaggi quali Bill Gates e Steve Jobs, in realtà queste figure, sicuramente importantissime per la diffusione capillare dell'informatica, non ebbero altrettanto peso nei passi pionieristici fondamentali. Esiste infatti una nutrita schiera di personaggi, ai più sconosciuti, che ha scritto le pagine più importanti dell'informatica.

Tra tutti, la pagina più incredibile è quella di una donna, Ada Lovelace[6] (1815-1852: il secolo precedente, non avete letto male!), nipote di Lord Byron. Costei, decenni prima che il computer fosse inventato o anche solo concepito, ha immaginato e definito il concetto e i primi formalismi della programmazione, cioè l'anima che avrebbe trasformato la "macchina elettronica" (il computer!) in qualcosa capace di eseguire compiti sofisticati di vario tipo.

Senza Ada Lovelace (le cui intuizioni hanno dell'incredibile, provate a pensarci) il computer non esisterebbe e il nostro mondo probabilmente sarebbe oggi molto diverso.

Era una giovane donna della metà dell'Ottocento, con la passione per la matematica. Quando ho letto di lei, mi ha colpito l'apparente leggiadria e quasi frivolezza dell'immagine che si trova nei libri: vestitino d'epoca vittoriana, gonna con le stecche di balena per renderla ampia, dotazione di pizzi, ombrellino parasole, ventaglio. Difficile pensare che questa donna fosse avanti almeno di un secolo rispetto al suo tempo, riuscendo a concepire qualcosa di incredibilmente astratto (a quel tempo) ma terribilmente concreto (oggi, a più di un secolo dalla sua morte) come la programmazione di un computer!

Pochi ne hanno sentito parlare in questi termini (voi non la conoscevate, vero?) e molti ritengono ben più rilevanti i contributi di altri personaggi recenti, magari diventati famosi anche per le ricchezze ac-

6 Ada Lovelace descritta su Wikipedia: https://it.wikipedia.org/wiki/Ada_Lovelace

cumulate grazie a politiche commerciali accorte. Un linguaggio di programmazione particolarmente sofisticato e potente ha ricevuto il suo nome, il linguaggio ADA.

Qualcuno si è dimenticato di citarla, di pubblicizzarla, di esaltarne la bravura e la lungimiranza. Forse perché donna, a quel tempo impossibile presenza in un laboratorio?

Dimenticanze che avvengono anche per tante altre donne che, con maggiori difficoltà degli uomini, hanno saputo calcare la scena delle tecnologie e tracciare strade vitali per il nostro futuro.

Che il computer e l'informatica avessero un'anima e un DNA indiscutibilmente femminile si è poi capito anche grazie ad altre gloriose donne[7] che col computer hanno compiuto imprese storiche, anche se nessuna (è un mio personale giudizio) così "alta" e "futuristica".

Ad Ada Lovelace, in particolare, dobbiamo quindi dire grazie.

Oltre a gettare le basi per la programmazione, la sua collaborazione con Lord Babbage[8] permise da una parte di risolvere vari problemi teorico-pratici che lo studioso aveva con la "macchina analitica" (il primo modello di calcolatore, in pratica) ma dall'altra prefigurò aspetti futuristici dell'informatica, quali quelli dell'*intelligenza artificiale*.

Siamo su un altro pianeta, quando si parla di Ada.

Lo scenario tecnologico

I computer sono dappertutto, non solo nelle forme classiche che tutti conoscono. Ce ne sono anche di camuffati sotto mentite spoglie: lo smartphone, per esempio, è un computer. Anche i televisori, le radio e tanti elettrodomestici (praticamente tutti, oggi) ne hanno dentro almeno uno. Un monopattino elettrico, un'auto; treni, aerei e navi. Satelliti. L'orologio da polso. L'asciugacapelli e l'aspirapolvere. Tutti que-

7 La storia di Katherine Johnson è un classico esempio, tra tantissimi, dove alla difficoltà di essere donna se ne aggiunge un'altra, quella di essere di colore. Un bellissimo film ce ne ricorda la storia: https://it.wikipedia.org/wiki/Il_diritto_di_contare

8 https://it.wikipedia.org/wiki/Charles_Babbage

sti oggetti, grazie al computer, funzionano e fanno quello che serve. Anche ciò che fino a un certo tempo funzionava senza computer (un aspirapolvere, un asciugacapelli, un forno elettrico, una lavatrice, per fare degli esempi) adesso ha un computer dentro! Come se non potesse esserne privo per effetto di una moda. Perfino l'acquario con i pesci tropicali ha un computer che controlla la temperatura dell'acqua e interviene "nel caso".

Altri computer, sempre "camuffati da qualcos'altro", supervisionano il pacemaker, strumento che, grazie all'informatica, oggi controlla in continuazione il battito del cuore, rilevandone anche i difetti più lievi. Li registra nella sua memoria, dove il medico (via wireless, quindi senza far buchi, tagli o utilizzare sondini) potrà leggerne la storia delle anomalie. Il pacemaker ha anche capacità di prendere decisioni importanti, quali per esempio quella di "obbligare" il cuore a battere col giusto ritmo, anche quando per qualche motivo chimico o nervoso il cuore vorrebbe battere all'impazzata o, al contrario, vorrebbe fermarsi o battere con un andamento jazzistico molto pericoloso per la nostra salute.

Ecco: cosa accadrebbe se un hacker mettesse le mani su un pacemaker attivo nel nostro corpo? Potrebbe uccidere qualcuno?[9] Quei robot che "vanno in giro" all'interno del nostro corpo[10] per fare sofisticati interventi cosa potrebbero combinare nel caso un hacker riuscisse ad accedervi?

Nella maggior parte dei casi i computer aiutano tanti tipi di strumenti, meccanismi o dispositivi a funzionare meglio, a essere più sicuri, a recepire cosa sta succedendo, a prendere delle decisioni importanti. A fermare un mezzo che sta per esempio andando a collidere con un ostacolo.

State bruciando il cibo? Il forno potrebbe avere un sensore di fumi che se ne accorge e il computer, programmato appositamente, potrebbe spegnere il forno, evitando danni peggiori!

---

9 Il pacemaker di Dick Cheney, vicepresidente degli USA, nel 2007 è stato modificato, spegnendo l'interfaccia wireless nel timore di un attentato fatto da un hacker! https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html

10 https://www.slashgear.com/777282/these-injectable-nanobots-can-walk-around-inside-a-human-body/

La centrifuga della lavatrice è sempre stata oggetto di storie al limite dell'incredibile. Lavatrici che saltellano qua e là, assatanate, nel voler per forza assolvere al compito di far girare il cesto della biancheria al massimo della velocità, anche quando il carico nel cestello è sbilanciato. Un computer con un sensore di vibrazione potrebbe ridurre la velocità di rotazione ed evitare questa danza. Il computer nella lavatrice potrebbe fare altro (e in molti casi lo fa), per esempio far girare preventivamente il cestello in modo da assestare il carico nel modo migliore, per poi poter lanciare una centrifuga perfetta, senza vibrazioni e senza quei piccoli viaggi che a volte compiono, con un suono da aereo al decollo! Ci ha pensato il computer. Una volta ci voleva il domatore di lavatrici, avvinghiato alla stessa nel tentativo di contenerne i movimenti!

Ma i computer talvolta non sembrano sempre delle docili e intelligentissime balie. A volte eseguono docilmente gli ordini ricevuti ma, come ormai abbiamo sperimentato in varie occasioni, c'è sempre qualcosa in agguato: l'imponderabile. Siete poco pratici dell'oggetto, per sbaglio avete cliccato tre millimetri a sinistra e attivato l'autodistruzione di qualcosa… e guarda caso manca il tasto "*Mi sono sbagliato*"! Vi precipitate a tentare di spegnere l'infernale strumento, ma non c'è niente da fare: il computer è veloce, mediamente, ma lo è in modo particolare quando sta combinando un guaio!

La password

Ma non è l'unico rischio che corriamo, usando queste strane macchine. Uno dei rischi più grandi è quello legato a quel riquadro in cui ci viene indicato il messaggio: "*Inserire la password*".

Mediamente, ricordarsi la password in tempo utile è come vincere alla lotteria… accidenti a chi l'ha inventata, questa password (e magari l'avete inventata voi). La password la sapete, la ricordate perfettamente, ma il computer ha un'opinione diversa. Insistete, cocciutamente, ma non c'è niente da fare. Tra l'altro, insospettiti dal fatto che siete al trentaquattresimo tentativo infruttuoso, il computer (che è proprio

stupido a non capire che siete voi!) comincia a pensare che potreste essere qualcun altro, un furbone che prova a indovinare la password e quindi decide di "fare resistenza".

"*Sai che c'è? Secondo me non sei tu, sei qualcun altro! Non ti bado più! Rivolgiti all'amministratore di sistema, che ti sistemerà lui!*".

```
L'inventore della password sicuramente sta bruciando
all'inferno, nell'immaginario collettivo! Però il
controllo della password è indispensabile per evitare
che qualcun altro entri nei nostri account o nel
nostro computer e che, oltre a farsi gli affari
nostri, possa spacciarsi per noi, causando gravi
problemi.
```

Così chiamate un tecnico. Se il fatto è accaduto in azienda, il tecnico appena vede il vostro numero di telefono sa già che vi siete dimenticato la password. Impietosamente vi guarda con quell'odioso sorrisetto (lo vedete anche se vi chiama per telefono, invece di arrivare di persona!) del tipo "*uno più imbranato di te non l'ho mai visto*"… Uno strazio di situazione che sapete già che si ripeterà enne volte. Situazione che non potete che odiare profondamente, come, del resto, vi verrebbe da odiare quella dannata scatola che ha software di intelligenza artificiale, ma non capisce che siete voi a volerla usare!

Se invece sperate di potervi arrangiare, allora immaginate che si debba reimpostare la password ma lo strumento infernale non vi lascia usare quella vecchia, vi tocca inventarne un'altra. L'ennesima.

Avete da tempo già utilizzato i nomi di familiari, di fidanzate, dei figli, una parolaccia, il cantante preferito o la grappa di fiducia. Le date di nascita che vi potreste ricordare non sono molte. La squadra di calcio preferita o qualche atleta di rilievo sono già stati usati. Come cavolo potete inventare una password nuova senza incappare nell'enorme rischio che dopo dieci minuti che l'avete inventata ve la

siete già dimenticata? Un problema senza soluzione!!! E così vi spaccate la testa per inventare l'ennesima password "nuova" e vi sembra tale. La inserite, ma il computer vi dice "*Non puoi usare password vecchie!*". Ci sono computer che son finiti nella spazzatura per molto meno!

Se avete vissuto qualcosa del genere, allora, sappiatelo… ci siamo passati tutti!!!

Vedremo più avanti qualche possibile suggerimento, anche se non ci sono formule magiche, sappiatelo!

Maneggiare informazioni

Ma a cosa serve l'informatica? Beh, a maneggiare le informazioni.

Il termine "maneggiare" comprende diverse attività specifiche, tra cui immagazzinare, elaborare, trasmettere, ricevere, copiare, cancellare, modificare. Ma anche rendere selettive queste operazioni, in modo che Tizio non possa "maneggiare" informazioni che appartengono a Caio.

L'informatica ha gradualmente reso molto più sofisticati ed efficienti i primi rudimentali strumenti realizzati da pionieri geniali, passando da una attività di sviluppo artigianale a un modello ampiamente strutturato e organizzato.

L'evoluzione industriale dell'informatica ha permesso una rapida diffusione di strumenti informatici sofisticati, contribuendo a renderli strumento comune di lavoro e di supporto a qualunque tipo di attività umana. Dal manipolo di informatici in camice bianco, con un pacco di schede perforate in mano, abili a comunicare con queste macchine complicatissime e grandi come armadi a quattro ante (tecnici che venivano formati con anni di studio specifico), si è passati al computer usato agevolmente dai bambini delle scuole elementari per fare i compiti o per giocare.

La rivoluzione ha cambiato anche il nostro modo di conoscere, perché cinquant'anni fa si imparava sui libri o andando a lezione da qualcuno. Oggi trovi tutto in internet.

Le capacità di elaborazione sono passate da quelle di una potente calcolatrice alla possibilità di simulare il comportamento di un aereo in volo, effettuando milioni di complesse elaborazioni geometriche, fisiche, grafiche al secondo.

Anche la capacità di gestire dati ha fatto una evoluzione incredibile. Ricordo la memoria a 64 bit, grande quasi come una valigia. Aveva 64 circuiti elettronici, ognuno serviva per "ricordare" un valore "0" o "1". Consumava decine di watt. Poi siamo passati a memorie digitali su circuiti integrati; ricordo un circuito integrato grande qualche centimetro con spazio da 2 kbyte (come dire 2000 caratteri). Sembrava uno spazio enorme. Adesso la più banale chiavetta USB contiene decine o centinaia di miliardi di "celle".

I sistemi di memorizzazione son passati dai nastri alle cassette audio, con cui un testo di una pagina si recuperava dal nastro in qualche minuto di paziente attesa. In un'audiocassetta ci stavano perfino 100 kbyte (!). Poi sono arrivati i floppy disk, da poche decine di kilobyte a quasi 2 megabyte (2 milioni di caratteri) nelle loro migliori realizzazioni. E infine i dischi rigidi, inizialmente con qualche decina di megabyte di spazio e dal costo equivalente di decine di migliaia di euro, dal consumo di qualche kilowatt. Oggi un disco da mille miliardi di caratteri (un terabyte!) è considerato di dimensione medio-bassa, costa qualche decina di euro e consuma qualche watt. E con la capacità di elaborazione e conservazione di quantità consistenti di dati, si è sempre più concretizzata la possibilità di trasportare ed elaborare (dopo averli convertiti in dati numerici, la cosiddetta "campionatura") suoni e immagini, facendo poi l'operazione inversa per riottenere audio e immagini originali.

Così i computer hanno permesso di ascoltare voce e musica, vedere immagini e filmati. Altra rivoluzione epocale.

A questa crescita impressionante della disponibilità di spazi di memorizzazione si è accompagnata una parallela tendenza "al consumismo", per cui le tecnologie si sono "allargate" a dismisura nei consumi di spazio. Giusto per fare un esempio, una lettera di qualche pagina inizialmente consumava pochi kilobyte (poche migliaia di caratteri/

byte) mentre oggi la stessa lettera con lo stesso contenuto (magari con qualche effetto grafico accattivante) consuma un centinaio di volte lo spazio originale!

Discorso analogo anche per i programmi. Mi ricordo programmi fatti personalmente con dimensioni di un kilobyte (mille caratteri/byte) che, dati oggi in pasto a un moderno strumento di programmazione, senza nulla modificare o aggiungere, acquistano una dimensione impensabile allora, occupando trecento o quattrocento kilobyte.

Per anni i primi sistemi operativi dei personal computer (parliamo degli anni ’80) avevano delle dimensioni complessive di qualche centinaio di kilobyte. Oggi Windows, anche nella sua versione più risparmiosa, occupa qualche decina di gigabyte (migliaia di volte più grande!).

E che dire della memoria RAM, quella specie di “scrivania” in cui il computer può maneggiare a velocità altissima i soli dati da manipolare, lasciando il resto dei dati non immediatamente necessari sul disco? due kbyte di RAM per i primi computer “seri” degli anni ’70-’80; adesso otto miliardi di byte non si negano a nessuno, nemmeno allo smartphone (una saggia considerazione: la memoria, quale che sia, non basta mai e si riempie sempre al 99 per cento, per cui si rende sempre necessario aumentarla)!

Per quanto riguarda le capacità comunicative, semplificando il discorso possiamo citare alcuni numeri: una comunicazione via radio permetteva di spedire qualche decina di caratteri al secondo (!), sempre se le condizioni di campo radio erano decenti.

Prestazioni analoghe erano presenti nei primi terminali connessi a computer. Negli anni ’70 si videro le prime comunicazioni informatiche a velocità dieci volte superiori, in grado di viaggiare tramite modem sulla rete telefonica tradizionale (i dati da spedire venivano trasformati dal modem in suoni e il modem ricevente li ritrasformava in dati).

Le velocità aumentarono rapidamente quando, invece di usare frequenze acustiche per trasportare i dati, si usarono onde radio a frequenze molto più alte dei segnali acustici telefonici (arrivavano a 3

kHz). Con le ADSL la frequenza era centinaia di volte più alta, quindi molto maggiori erano le velocità praticabili sui cavi telefonici. Sempre con segnali radio ad alta frequenza (dell'ordine delle decine o centinaia di MHz) si effettuano le trasmissioni dati sulle reti locali aziendali. Infine con le fibre ottiche la frequenza utilizzata per la trasmissione (milioni di volte superiore) permette velocità incredibili e notevoli distanze, anche grazie alla ridottissima dispersione del segnale (essendo ottico ed essendo la fibra ottica dotata di capacità riflettenti, il segnale non si disperde).

I segnali radio, però, non sono passati di moda, anzi. Le connessioni, infatti, viaggiano via radio in tanti modi:

- Tramite ponti radio tra zone diverse (es. tra una città e l'altra)
- Via radio tramite satelliti (vecchio tipo o Starlink)
- Via radio tramite telefonia mobile (tethering o modem GSM)
- In aree ristrette e all'interno di uffici (wireless)
- Bluetooth, per brevissime distanze (sotto i 10 metri)

Ma i server non c'erano

Prima della rete internet attuale, verso la fine degli anni '70, si diffusero sempre più i BBS (Bulletin Board Service).[11] Oggetti telematici molto simili (con le limitazioni del tempo) ai nostri attuali server. Ci si connetteva a un BBS per trovare documenti, testi, ricerche. Sui BBS si potevano depositare dei file e permettere ad altri di scaricarli. Uno o più sysop (amministratori del BBS) moderavano i contenuti, gli accessi e gli abusi.

Verso la fine degli anni '80 i BBS raggiunsero una diffusione notevole. Molti tra loro si coordinarono, sia tecnicamente che dal punto di vista dei contenuti, per cui in piccolo si era creata già allora quella che poteva assomigliare a una piccola rete internet.

11 I BBS descritti su Wikipedia: https://it.wikipedia.org/wiki/Bulletin_board_system

Ovviamente solo una parte ridotta della popolazione poteva accederci, vista la scarsa (allora) diffusione dei computer.

I BBS hanno comportato la nascita delle “anomalie”, oggi esistenti in internet, per quanto riguarda gli hacker e i reati informatici. Nei BBS si trovavano programmi copiati illegalmente. Anche le tipologie di documenti potevano allontanarsi notevolmente dal lecito, in quanto a tipologie di contenuti e riservatezza. Alcune BBS contenevano documenti derivanti da furti e con i BBS si sviluppò notevolmente anche la pedofilia online. I BBS furono anche le prime vere palestre per gli hacker e diedero spazio alla maggior parte dei reati informatici che oggi troviamo in Rete.

Alcuni BBS hanno implementato praticamente anche i primi esempi di “luoghi pirata” (analoghi all’attuale Dark Web), fornendo spazi di incontro per pirati informatici i quali praticavano ogni tipo di commerci illeciti esistenti.

Sempre tramite i BBS si svolsero i primi “combattimenti informatici” e anche i servizi segreti di molti paesi (e varie strutture militari) usavano i BBS per le loro attività.

I BBS in pratica costituirono il primo robusto esempio di utilizzo ampio e articolato degli strumenti informatici e delle attività in rete, sia in senso positivo (crescita della cultura informatica, incremento della popolazione, condivisione di documentazione tecnica e formativa, collaborazione tra informatici, laboratori condivisi eccetera), sia in senso negativo (software pirata, reati informatici di vario tipo, dati personali di terzi).

Nei primi anni ’90, anche in Italia, i BBS cominciarono ad avere una notevole diffusione. Una delle reti di BBS più conosciuta era FidoNet, che raggruppava qualche centinaio di BBS.